KAMUDA BULUT BİLİŞİM KULLANIMINA YÖNELİK RİSK ANALİZİ VE YÖNETİMİ

– UZMANLIK TEZİ –

HAZIRLAYAN: HAKAN KILIÇ

ANKARA – 2017

T.C.
ÇEVRE VE ŞEHİRCİLİK
BAKANLIĞI

KAMUDA BULUT BİLİŞİM KULLANIMINA YÖNELİK RİSK ANALİZİ VE YÖNETİMİ

Tezi Hazırlayan: Hakan KILIÇ

Tez Danışmanı : Ahmet DAŞKIN

Birim Amiri : Ömer ALAN

Hakan KILIÇ tarafından hazırlanan Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analizi ve Yönetimi adlı bu tezin Çevre ve Şehircilik Uzmanlık tezi olarak uygun olduğunu onaylarım.

Çevre ve Şehircilik Uzmanı Ahmet DAŞKIN
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Çevre ve Şehircilik Uzmanlık tezi olarak kabul edilmiştir.

Ömer ALAN
Başkan : Genel Müdür V.

Yrd. Doç. Dr. Hüseyin BAYRAKTAR
Üye : Genel Müdür Yardımcısı

Birol ÖZCAN
Üye : Daire Başkanı V.

Sibel ASLAN
Üye : Daire Başkanı V.

Ahmet DAŞKIN
Üye : Çevre ve Şehircilik Uzmanı

Bu tez, Çevre ve Şehircilik Uzmanlığı Tez Hazırlama Yönergesi'ne uygundur.

İÇİNDEKİLER

DIŞ KAPAK .....

İÇ KAPAK..... i

KABUL VE ONAY SAYFASI ii

İÇİNDEKİLER iii

ÖZET vii

ABSTRACT ix

TEŞEKKÜR xi

TABLO LİSTESİ xii

ŞEKİL LİSTESİ xv

RESİM LİSTESİ xvi

KISALTMALAR xvii

TANIMLAR xix

GİRİŞ 1

BÖLÜM 1

BULUT BİLİŞİMİN TEMELLERİ

1.1. Bulut Bilişim Nedir?..... 8

1.2. Bulut Bilişim İle İlgili Temel Kavramlar..... 9

1.2.1. Bulut bilişimin temel özellikleri.....9

1.2.2. Bulut bilişim benzeri teknoloji ve kavramlar.....13

1.3. Bulut Bilişimin Gelişimi ve Tarihçesi..... 20

1.4. Bulut Bilişim Servis Modelleri..... 24

1.4.1. Servis olarak Yazılım (SaaS)..... 25

1.4.2. Servis olarak Yazılım Geliştirme Platformu (PaaS)..... 27

1.4.3. Servis olarak Altyapı (IaaS)..... 29
1.4.4. Diğer Bulut Bilişim Servis Modelleri..... 30

1.5. Bulut Bilişim Mimari Çeşitleri..... 31

1.5.1. Açık (Public) Bulut..... 32
1.5.2. Özel (Private) Bulut..... 33
1.5.3. Hibrit (Hybrid) Bulut..... 34
1.5.4. Topluluk (Community) Bulutu..... 36

1.6. Bulut Bilişim Donanım ve Yazılım Katmanları 36

1.6.1. Bulut Bilişim Donanım Katmanı..... 37
1.6.2. Bulut Bilişim Yazılım Katmanı..... 38

1.7. Bulut Bilişim Kullanım Metotları..... 44

1.8. Bulut Bilişimin Getirdiği Avantajlar ve Riskler..... 50

1.8.1. Avantajlar..... 50
1.8.2. Riskler..... 54

1.9. Bulut Bilişim SWOT Analizi..... 58

BÖLÜM 2

BULUT BİLİŞİM İLE KAMU HİZMETLERİNİN ENTEGRASYONU

2.1. Bulut Bilişim İle İlgili Dünya Örnekleri..... 67

2.2. Ülkemizde Bulut Bilişim..... 80

2.3. Entegre Kamu Hizmetleri İçin Gereksinimler ve Bulut Çözümleri..... 95

2.3.1. Entegre Kamu Hizmetleri İçin Gereksinimler..... 96
2.3.2. Entegre Kamu Hizmetleri İçin Bulut Çözümleri..... 101

2.4. Kamu Bulutu İşletme Modelleri.....107

2.5. E-Devlet Hizmet ve Uygulamalarının Buluta Aktarılması.....112

2.5.1. Strateji Tanımlama..... 114
2.5.2. Mevcut Mimariyi Belirleme ve Anlama..... 115
2.5.3. Buluta Aktarım Planı Hazırlama..... 117
2.5.4. Sağlayıcı Seçimi..... 120
2.5.5. Analiz ve Test..... 121
2.5.6. Haritalama..... 126
2.5.7. Aktarma ve Yönetim..... 126

2.6. Kamuda Bulut Bilişim Kullanımının Faydaları ve Sorunlar..... 126

2.6.1. Kamuda Bulut Bilişim Kullanımının Faydaları..... 126
2.6.2. Kamuda Bulut Bilişim Kullanımına Yönelik Sorunlar..... 132

2.7. Kamuda Bulut Kullanımı İle İlgili Modeller ve Çözüm Önerileri..... 136

2.7.1. Kamuda Bulut Kullanımı İle İlgili Modeller..... 136
2.7.2. Kamuda Bulut Kullanımı İle İlgili Çözüm Önerileri..... 141

BÖLÜM 3

BULUT BİLİŞİM RİSK ANALİZİ

3.1. Risk, Risk Analizi ve Risk Yönetimi..... 156

3.2. Bulut Bilişimde Varlıkların Belirlenmesi ve Modellenmesi..... 157

3.2.1. Bulut Bilişimde Varlıkların Belirlenmesi..... 157

3.2.2. Bulut Bilişimde Varlıkların Modellenmesi..... 159

3.3. Bulut Bilişimde Tehdit ve Zafiyetler..... 163

3.3.1. Bulut Bilişime Özel Tehditler..... 163

3.3.2. Bulut Bilişime Özel Olmayan Tehditler..... 171

3.4. Bulut Bilişimde Riskler..... 178

3.4.1. Kurumsal ve Stratejik Riskler..... 179

3.4.2. Teknik Riskler ve Güvenlik Riskleri..... 185

3.4.3. Hukuksal Riskler..... 191
3.4.4. Buluta Özgü Olmayan Diğer Riskler..... 193
3.5. Bulut Bilişimde Risk Olasılık Değerlendirmesi..... 196
3.6. Bulut Bilişimde Risk Etki Analizi..... 202
3.7. Bulut Bilişimde Risk Değerlerinin Bulunması..... 210
BÖLÜM 4
BULUT BİLİŞİM RİSK YÖNETİMİ
4.1. Bulut Bilişim Risk İşleme..... 215
4.1.1. Uygun Kontrollerin Belirlenmesi..... 216
4.1.1.1. Teknik Güvenlik Kontrolleri..... 216
4.1.1.2. Yönetimsel Kontroller..... 219
4.1.1.3. Operasyonel Kontroller..... 220
4.2. Bulut Bilişim Risklerinin Kabul Edilebilirlikleri..... 221
4.3. Bulut Bilişim Risklerinin Değerlerinin Azaltılması, Transferi veya Risklerden Kaçınılması..... 228
4.4. Bulut Bilişim Risk İşleme Maliyet Analizi..... 261
4.5. Bulut Bilişimde Risk İzleme ve Değerlendirme..... 264
4.6. Bulut Bilişim Risklerinin Profilleri..... 266
KAYNAKLAR..... 294
ETİK KURALLARA YGUNLUK BEYANI..... 305
ÖZGEÇMİŞ..... 306

ÖZET

ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI	
Tezin Adı	Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analizi ve Yönetimi
Türü	Uzmanlık Tezi
Yazar	Hakan KILIÇ
Teslim Tarihi	17.01.2017
Anahtar Kelimeler	Bulut bilişim, risk yönetimi, kamu bulutu, risk işleme, veri merkezi
Tez Danışmanı	Ahmet DAŞKIN
Sayfa Adedi	306

20. yüzyılın ikinci yarısında belli bir ölçekte gerçekleşen bilişim sistemlerindeki gelişim, 21. yüzyılın ilk çeyreğinde önemli ölçüde hız kazanmış; yazılım ve donanım bileşenlerinde sağlanan teknolojik yenilik ve değişimler ile birlikte kullanıcı taleplerinin yoğunluğunda ve çeşitliliğinde yaşanan hızlı artış, bilişim mimarilerinde yeni metodolojilerin kullanılmasını zorunlu hale getirmiştir. Sanallaştırma, servis odaklı mimari, sunucu-istemci modeli, dağıtımlı hesaplama vb. öncül teknoloji ve kavramların gelişimi ve bütünleşmesiyle ortaya çıkan bir hizmet modeli olan bulut bilişim; kullanıcılarına düşük maliyetli, esnek, ölçülebilir, ölçeklendirilebilir, platform bağımsız erişilebilir ve yüksek performansa sahip mimariler sunar.

Eş zamanlı olarak çok sayıda kullanıcıya aynı platform üzerinden hizmet sunma imkânı sağlayan bulut bilişim mimarileri önce büyük çaplı özel sektör kuruluşlarının ve hemen ardından kamu kurum ve kuruluşlarının dikkatini çekmiş ve ilgili kamu kuruluşları vatandaşlara daha kolay erişilebilir, güvenli ve kullanılabilir bir şekilde hizmetlerini sunmak için bulut servis modellerini kullanma yoluna gitmişlerdir. Kamu kurum ve kuruluşlarının veri gizliliği içeren belli veri ve uygulamalarını kurum dışına aktaramaması kısıtlaması, birçok kuruluşun kullanımı için hem özel hem de açık bulut mimarisinin bir bileşkesi olan hibrit bulut mimarisini öne çıkarmaktadır. Yine birçok kamu kuruluşunun sunduğu hizmetlerin diğer kuruluşların servis edecekleri verilere ihtiyaç duyması geniş çaplı kamu bulutlarını kurmayı; pahalı yatırım ve işletme maliyetleri ile uzman bilişim personeli istihdamında yaşanan sorunlar her kamu kuruluşunun kendi veri merkezini kurması yerine entegre kamu veri merkezleri oluşturmayı zorunlu kılmaktadır. Bu doğrultuda gerek ülkemizde gerekse de dünyanın çeşitli ülkelerinde merkezi ve yerel yönetimler bazında ortak kamu

bulutları oluşturma ve entegre veri merkezleri kurma çalışmaları devam etmektedir.

Sağladığı birçok faydanın yanında bulut bilişim gerek sağlayıcı ve gerekse de müşterileri açısından birçok risk barındırmaktadır. Bu risklerin kuruluşlara verebileceği zararların minimize edilmesi veya ortadan kaldırılması için her kuruluşun kendine özgü bir risk yönetim modeli oluşturması hayati önem taşımaktadır. Bu doğrultuda kuruluşlar bulut bilişim mimarisindeki varlıklarını, bu varlıkların maruz kaldığı tehdit ve açıkları ve bunların sebep olduğu riskleri belirlemelidir. Belirlenen risklerin olasılık ve etki değerlerinin bulunarak, ilgili risk değerinin hesaplanmasının ardından; risk derecesine göre sırlanan risklerin risk işleme sürecine tabi tutulması gerekmektedir. Bu süreçte risk derecesi düşük riskler sürekli izlenmek ve varsa gerekli risk azaltıcı önlem ve kontrolleri uygulamak suretiyle kabul edilebilirken; göreceli olarak risk derecesi yüksek riskler için gerekli azaltıcı önlem ve kontrollerin uygulanması ve eğer varsa farklı kuruluşlara risk transferi yapılması veya ilgili riskten kaçınmak için riski oluşturan hizmetin hepsinin veya belli kısmının devre dışı bırakılması yöntemlerinin uygulanması zorunludur. İlgili risk azaltıcı kontrollerin uygulanabilirliğinin kontrolü açısından risk işleme maliyet analizleri ve ayrıca değişen teknolojilere, kuruluşların yeni operasyonlarına ve dolayısıyla yeni risklerine göre risk yönetim sürecinin güncellenebilmesi için risk izleme ve değerlendirme çalışmaları periyodik olarak gerçekleştirilmelidir.

ABSTRACT

MINISTRY OF ENVIRONMENT AND URBANIZATION	
Thesis	Risk Analysis and Management for the Use of Cloud Computing in the Public
Type	Expertise Thesis
Author	Hakan KILIÇ
Submission Date	17.01.2017
Key Words	Cloud computing, risk management, public cloud, risk mitigating, data center
Advisor	Ahmet DAŞKIN
Total Page	306

The development of information systems in a certain scale in the second half of the 20th century, have gained significant acceleration in the first quarter of the 21st century; technological innovation and changes in software and hardware components with the the rapid increase in the intensity and variety of user requests, has made the use new methodologies in information system architectures. Cloud computing, which is a service model that emerges with the development and integration of preliminary technologies and concepts such as virtualization, service-oriented architecture, server-client model, grid computing; provides low cost, flexible, scalable, platform independent accessible, and high-performance architectures to its users.

Cloud computing architectures that enable simultaneous service provision to multiple users across the same platform, firstly attracted the attention of large private sector organizations and then public institutions and organizations and related government agencies have begun to the use of cloud service models to provide their services to citizens more easily accessible, secure and usable. The restriction that public institutions and organizations can not transfer certain data and applications containing confidential data outside the institution, puts forward the hybrid cloud architecture for the use of many organizations, which is a combination of both private and public cloud architectures. Also, the need of data to be provided by other institutions to the services provided by many public institutions requires to build large scaled public clouds; expensive investment and operating costs and problems experienced in the employment of expert personnel necessitates to create integrated public data centers instead of each public entity to establish its own

data center. In this direction, both in our country and in various countries of the world, efforts to create common public clouds and to establish integrated data centers are continuing in central and local governments.

In addition to the many benefits it provides, cloud computing has many risks in terms of both providers and customers. It is vital that each organization establish a unique risk management model to minimize or eliminate the harms that these risks may cause to the organization. In this direction, organizations are able to identify their assets in the cloud computing architecture, the threats and vulnerabilities that these assets are exposed to and the risks that they cause. After determining the probability and impact values of the identified risks and calculating their related risk value; the risks that are classified according to their risk levels must be subjected to the risk mitigating process. In this process, low level risks can be accepted by continuous monitoring and if necessary implementing risk-reducing measures and controls. But for relatively high level risks, the implementation of necessary mitigation measures and controls and if applicable it is obligatory to apply the methods of transfering risk to different institutions or disabling all or part of the service that creates the risk to avoid the related risk. Risk mitigating cost analysis in terms of control of the feasibility of the relevant risk reduction controls and also risk monitoring and evaluation studies to update the risk management process according to changing technologies, new operations of organizations and therefore new risks; should be carried out periodically.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren tez danışmanım Çevre ve Şehircilik Uzmanı Sn. Ahmet DAŞKIN'a. Tezimi baştan sona dikkatle inceleyen ve yapıcı eleştirileriyle çalışmaya şekil ve içerik yönünden katkı sağlayan Tez Jürisi Başkanı ve üyelerine. Manevi destekleriyle beni hiçbir zaman yalnız bırakmayan başta Belgelendirme ve Yaygınlaştırma Daire Başkanlığı çalışanları olmak üzere tüm mesai arkadaşlarıma ve ayrıca tez çalışması süresince kendilerine yeteri kadar zaman ayıramasam da, her daim yanımda durarak bana manevi güç veren başta eşim ve çocuklarım olmak üzere tüm aileme teşekkürü bir borç bilirim.

Hakan KILIÇ

TABLO LİSTESİ

Tablo.1.1: Bulut Bilişim SWOT Analizi..... 65

Tablo 2.1: 2016 BSA Global Bulut Bilişim Puan Çizelgesi..... 68

Tablo 2.2: E-Devlet ve C-Devlet..... 96

Tablo 3.1: Bulut Bilişim Varlık Listesi..... 161

Tablo 3.2: Bulut Bilişim Varlıkları Süreç Modellenmesi..... 163

Tablo 3.3: Risk Olasılıkları..... 197

Tablo 3.4: Risk Etkileri..... 203

Tablo 3.5: Risk Derecelendirme Matrisi..... 211

Tablo 3.6: Risk Dereceleri ve Tanımları..... 212

Tablo 4.1: Risk İşleme Seçenekleri..... 222

Tablo 4.2: R.1-Yönetim ve Kontrol Kaybı Risk Profili..... 267

Tablo 4.3: R.2- Bulut Hizmeti Sonlandırması veya Arızası Risk Profili..... 268

Tablo 4.4: R.3- Servis Sağlayıcı Bağımlılığı Risk Profili..... 268

Tablo 4.5: R.4- Üçüncü Parti Tedarikçi Hatası Risk Profili..... 269

Tablo 4.6: R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması Risk Profili..... 269

Tablo 4.7: R.6- Uyum Sorunları Risk Profili..... 270

Tablo 4.8: R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı Risk Profili..... 270

Tablo 4.9: R.8- Dış Kaynaklı Saldırılar Risk Profili..... 271

Tablo 4.10: R.9- Verilerin Güvensiz veya Etkisiz Silinmesi Risk Profili..... 271

Tablo 4.11: R.10- Nakil Halindeki Veriyi Yakalama Risk Profili..... 272

Tablo 4.12: R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş Risk Profili…..…. 273

Tablo 4.13: R.12- Kaynak Tükenmesi Risk Profili..... 273

Tablo 4.14: R.13- Şifreleme Risk Profili..... 274

Tablo 4.15: R.14- Kaynak İzolasyonu Eksikliği Risk Profili..... 274

Tablo 4.16: R.15- Hizmet Kesintisi veya Bozulması Risk Profili..... 275

Tablo 4.17: R.16- Kötü Amaçlı Araştırma veya Taramalara Girişilmesi Risk Profili..... 275

Tablo 4.18: R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık Risk Profili..... 276

Tablo 4.19: R.18- Şifreleme Anahtarlarının Kaybı Risk Profili..... 276

Tablo 4.20: R.19- Hizmet Motorunun Hacklenmesi Risk Profili..... 277

Tablo 4.21: R.20- Yargı Değişiminden Kaynaklanan Riskler Risk Profili..... 277

Tablo 4.22: R.21- Mahkeme Celbi ve E-Keşif Risk Profili..... 278

Tablo 4.23: R.22- Veri Sansürü Risk Profili..... 278

Tablo 4.24: R.23- Lisans Riskleri Risk Profili..... 279

Tablo 4.25: R.24- Veri Koruma Riskleri Risk Profili..... 279

Tablo 4.26: R.25- Ayrıcalık Yükseltme Olasılığı Risk Profili..... 280

Tablo 4.27: R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması Risk Profili..... 280

Tablo 4.28: R.27- Ağ Kesilmeleri Risk Profili..... 281

Tablo 4.29: R.28- Sosyal Mühendislik Saldırıları Risk Profili..... 281

Tablo 4.30: R.29- Hizmet Ücreti Değişikliği Risk Profili..... 282

Tablo 4.31: R.30- Ağ Trafiğini Değiştirme Risk Profili..... 282

Tablo 4.32: R.31- Yedeklerin Kaybolması veya Çalınması Risk Profili..... 283

Tablo 4.33: R.32- Doğal Afetler Risk Profili..... 283

Tablo 4.34: R.33- Ağ Yönetimi Sorunları Risk Profili..... 284

Tablo 4.35: R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması Risk Profili..... 284

ŞEKİL LİSTESİ

Şekil 1.1: Bulut Bilişimde Platform Bağımsız Erişim..... 9

Şekil 1.2: Bulut Bilişim Servis Modelleri..... 25

Şekil 2.1: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Mobil Arayüzü (Android)..... 93

RESİM LİSTESİ

Resim 2.1: Çevre ve Şehircilik Bakanlığı Veri Merkezi..... 89

Resim 2.2: Çevre ve Şehircilik Bakanlığı Siber Güvenlik Operasyon Merkezi..... 90

Resim 2.3: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Web Giriş Arayüzü..... 91

Resim 2.4: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Web Arayüzü..... 92

Resim 2.5: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Masaüstü Arayüzü..... 93

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AKS : Adres Kayıt Sistemi

API : Uygulama Programlama Arayüzü (Application Programming Interface)

Ar-Ge : Araştırma ve Geliştirme

A.Ş. : Anonim Şirketi

BİT : Bilgi ve İletişim Teknolojileri

BSA : Uluslararası İş Yazılımları Birliği (Business Software Alliance)

BT : Bilgi Teknolojileri

BTYK : Bilim ve Teknoloji Yüksek Kurulu

CIO : Kıdemli Bilgi Yöneticisi (Chief Information Officer)

CSA : Bulut Güvenliği Ajansı (Cloud Security Ajansı)

DDoS : Dağıtılmış Hizmet Engelleme (Distributed Denial of Service)

DILA : Fransa Hukuki ve İdari Bilgiler Müdürlüğü

DPT : Devlet Planlama Teşkilatı

e-Devlet : Elektronik Devlet

EDOS : Ekonomik Sürdürülebilirlik Engelleme (Economic Denial Sustainability)

e-Ticaret : Elektronik Ticaret

ENISA : Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency)

GBit : Gigabit (1 milyar bite karşılık gelen bir hafıza birimidir.)

Gbps : Saniyede Aktarılan Gigabit Sayısı (Gigabits per second)

GSA : ABD Genel Hizmetler Dairesi (General Services Administration)

GSYH : Gayri Safi Yurtiçi Hasıla

IaaS : Servis olarak Altyapı (Infrastructure as a Service)

ISO : Uluslararası Standartlar Organizasyonu (International Standards Organisation)

ISRAM : İletişim Teknolojileri Risk Analiz Metodu (Information Security Risk Analysis Method)

KOBİ : Küçük ve Orta Büyüklükteki İşletme

LDAP : Basit İndeks Erişim Protokolü (Lightweight Directory Access Protocol)

Mbps : Saniyede Aktarılan Megabit Sayısı (Megabits per second)

MERNIS : Merkezi Nüfus İşletim Sistemi

NCSA : Ulusal Süperbilgisayar Uygulamaları Merkezi (National Center for Supercomputer Applications)

NIST : ABD Ulusal Standartlar ve Teknoloji Enstitüsü

OVF : Açık Sanallaştırma Biçimi (Open Virtualization Format)

OWASP : Açık Web Uygulama Güvenliği Projesi (Open Web Application Security Project)

PaaS : Servis olarak Platform (Platform as a Service)

RAM : Rastgele Erişim Belleği (Random Access Memory)

SaaS : Servis olarak Yazılım (Software as a Service)

SAN : Depolama Alanı Ağı (Storage Area Network)

SGK : Sosyal Güvenlik Kurumu

SLA : Hizmet Seviye Anlaşması (Service Level Agreement)

SMTP : Elektronik posta gönderme protokolü (Simple Mail Transfer Protocol)

SOA : Servis Odaklı Mimari (Service-Oriented Architecture)

SSL : Güvenli Soket Katmanı (Secure Sockets Layer)

TAKBİS : Tapu Kadastro Bilgi Sistemi

T.C. : Türkiye Cumhuriyeti

TSE : Türk Standartları Enstitüsü

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜRKSAT : TÜRKSAT Anonim Şirketi

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

UYAP : Ulusal Yargı Ağı Projesi

VPN : Sanal Özel Ağ (Virtual Private Network)

WAN : Geniş Alan Ağı (Wide Area Network)

TANIMLAR

API (Uygulama Programlama Arayüzü): Bir yazılımın başka bir yazılımda tanımlanmış işlevlerini kullanabilmesi için oluşturulmuş bir tanım bütünüdür. Kullanıcılara geliştirecekleri yazılım veya uygulama ile ilgili olarak gerekli program bloklarını, protokolleri, rutinleri ve araçları sunan programlardır.

Birlikte Çalışabilirlik: Bir sistemin, kişinin ya da sürecin, ortak standartlar çerçevesinde bir diğer sistemin, kişinin ya da sürecin bilgisini ve/veya işlevlerini kullanabilme yeteneğidir.

Bulut Bilişim Hizmet Sağlayıcısı: Müşterilerine bulut bilişim hizmeti sunan firma veya kuruluşlardır.

Çoklu Kiracılık: Bir uygulama örneğini birden fazla kiracı arasında paylaşmak için, uygulama üzerinde her kiracıya adanmış özel bir "pay" sağlayan, performans ve veri gizliliği açısından diğer paydaşların izole edildiği bir yaklaşımdır.

Dağıtımlı Hesaplama: Dağıtık bilgi işleme mimarisinin sanallaştırılmasını sağlayan çözüm mimarisine dağıtımlı hesaplama denilmektedir. Buradaki temel amaç dağıtık bilgi işleme ve veri kaynaklarının kullanmakta olduğu işlemci güçleri, ağ kapasiteleri ve depolama kapasiteleri ile tek büyük bir sistem yaratmaktır. Yaratılan bu sistem tamamen birbirinden bağımsız çalışmakta olan ve birbirine benzemeyen sistemlerin bir araya gelerek oluşturduğu sanal bir işleme gücüdür.

Dağıtık Mimari: Birden fazla bilgisayar ve/veya sunucunun birbirleri arasında iletişim kurması ve birbirleri ile replika şekilde bir ağ bütünü olarak çalışmasıdır.

İstemci-Sunucu Modeli: Sunucu adı verilen kaynak veya hizmet sağlayıcıları ile istemci denilen hizmet talep edenler arasında görev veya iş yükünü paylaştıran dağıtılmış uygulama yapısıdır. Burada sunucular kendi bilişim kaynaklarını istemciler ile paylaşırken, istemciler herhangi bir kaynak paylaşmayıp sadece sunucudaki içeriği veya sunulan hizmet uygulamasını talep ederler.

Kaynak Havuzu Oluşturma: Bulut sağlayıcısının farklı fiziksel ve sanal kaynaklarının birden çok tüketiciye hizmet verebilmek amacıyla, bir araya getirilerek dinamik müşteri talebine göre çoklu kiracılık modeli kullanılarak her bir müşteriye atanması, geri alınabilmesi ve tekrar atanabilmesidir.

Kullanım Bazlı Ücretlendirme: Sağlayıcıların kullanılan bilişim kaynağı miktarını ölçüp, bu miktarı birim kaynak kullanımı ile çarparak müşterilerinden ücret talep ettiği ücretlendirme modelidir.

Risk Yönetimi: Kuruluşların işlevleri sırasında ortaya çıkabilecek riskleri önceden dikkatli bir biçimde ve ayrıntıları ile tanımlayıp, değerlendirilmesi ve bu riskleri minimize edecek veya tam olarak ortadan kaldıracak önlemleri almasıdır.

Sağlayıcı Bağımlılığı: Bulut bilişimde farklı hizmet sağlayıcıların müşterilerini başka sağlayıcılara kaptırmamak için kendilerine özel protokoller, uygulama programlama arayüzleri, veri yapıları ve hizmet modelleri kullanması ve kullanılan bu yapıların diğer sağlayıcıların kullandıkları yapılarla uyumsuz olması sebebiyle; bir hizmet sağlayıcısından diğer bir hizmet sağlayıcısına geçişin zor olması ve tek bir hizmet sağlayıcısına bağımlı kalınması durumudur.

Sanallaştırma: Bilişim kaynaklarının (CPU, depolama, ağ, bellek, uygulama yığını ve veritabanı) hizmet tüketen uygulamalar ve son kullanıcılardan soyutlanarak mantıksal kaynaklara bölünmesi ve ortaya çıkan her bir mantıksal kaynağın farklı kullanıcılar tarafından ayrı birer fiziksel kaynak gibi kullanılmasıdır.

Servis odaklı mimari: Bilgisayar sistemlerinin işlevselliklerini iş süreçleri etrafında gruplaştırarak, sistem geliştirmesi ve bütünleştirilmesinde yol gösteren bir yazılım tasarımı felsefesidir.

Talep Üzerine Self Servis: Bir kullanıcının servis sağlayıcısı ile irtibata geçmeden sunucu kullanım süresi ve ağ depolama kapasitesi gibi bilişim kaynaklarını otomatik olarak ihtiyaç miktarına göre temin edebilmesidir.

Web 2.0: Gelişen iletişim ve ağ teknolojileri sayesinde, internet teknolojilerinin kullanıcı tarafından içerik oluşturulması, kullanışlılık ve birlikte çalışabilirlik vb. konularda gösterdiği gelişimi ifade eden bir terimdir.

GİRİŞ

Veri üretiminin, internet kullanımının ve dolayısıyla internet üzerinden veri paylaşımının hızla arttığı ve çeşitlendiği günümüzde, kullanıcı taleplerinin uygulamaları zaman, mekân ve platformdan bağımsız olarak kullanabilme yönünde gelişmesi; bulut bilişim kavramını hayatımızda her geçen gün daha önemli hale getirmektedir. Bulut bilişim genel olarak, asgari düzeyde bilişim yönetimiyle; ölçeklenebilir, ölçülebilir ve esnek bir şekilde bilişim kaynaklarının (ağlar, sunucular, depolama alanı, uygulamalar ve servisler gibi) paylaşılabilmesine, internet teknolojileri kullanılarak müşterilere servis olarak sunulabilmesine ve bu kaynakların müşteriler tarafından talep edilen ölçüde kullanımına olanak sağlayan bir bilişim hizmet modeli olarak tanımlanabilir. Tanımdan da anlaşılacağı üzere bulut bilişim, depolama ve veri işleme yükünü istemci bilgisayarlar üzerinden alıp, uzak sunucular üzerine aktaran bir hizmet modelidir. Sunucular üzerinde depolanan ve istemciler tarafından talep edilen işleme tabi tutulan veriler, ihtiyaç duyulduğu anda, internet üzerinden istemci bilgisayarlara aktarılırlar. Verilere platform bağımsız olarak, farklı lokasyonlardan internete bağlı herhangi bir istemci cihaz üzerinden erişilebilir.

Bulut bilişimin temel özelliklerini, herhangi bir ek uygulama veya eklentiye gerek kalmadan tüm hizmetin tarayıcı üzerinden sunulabilmesi ve kullanılabilmesi, ölçülebilir ve ölçeklendirilebilir yapısı sayesinde kullanılan kaynak miktarının esnek bir şekilde artırılabilmesi, artırılan miktarın iade edilebilmesi ve kullanılan kaynak miktarına göre ödeme yapılmasına olanak sağlaması, platformdan bağımsız olarak sadece tarayıcısı olan herhangi bir cihazdan erişime izin vermesi, sürekli çevrim içi yapısı sayesinde sürekli güncelleme imkânı sunması, çoklu dil desteği ile uluslararası düzeyde takım çalışmasına olanak sağlaması, bulut sağlayıcısının elindeki dağıtık mimarideki kaynaklardan bir kaynak havuzu oluşturarak çoklu kiralama mimarisi ile havuzdaki kaynaklarını çok sayıda müşterisine aynı anda kullandırabilmesine imkân

tanıması, yüksek disk kapasitesi, işlemci gücü, bant genişliği kullanabilmeye olanak sağlaması olarak sıralayabiliriz.

Bulut bilişimin mimarisinin ve uygulamalarının; maliyet, performans, hizmet kalitesi, esneklik, iş, zaman ve personel tasarrufu, güvenlik, birlikte çalışabilirlik ve uyum gibi konularda sağladığı avantaj ve faydalar, bu hizmet modelini kısa sürede önce özel sektör ve ardından da kamu sektörünün ilgi odağı haline getirmiştir. Temeli 1950'lere dayanan bulut bilişim kavramı, 2006 yılında Amazon firmasının Amazon S3 adlı ilk gerçek bulut bilişim hizmetini devreye almasıyla ticari olarak kullanılmaya başlanmıştır. İnternet üzerinden perakende satış yapan bu firma, yılın belli dönemlerinde artan müşteri talebi nedeniyle kurduğu geniş bilişim kaynağı altyapısının (sunucu, depolama ünitesi, ağ kaynağı vb.) yılın diğer dönemlerinde %90'a varan oranlarda atıl kalması nedeniyle, bu kaynakları kullandığın kadar öde prensibiyle kiralama yoluna gitmiş ve ağ üzerinden kullanılan verinin boyutu, kullanılan bant genişliği ve talep sayısına göre ücretlendirme politikası uygulamaya başlamıştır. Amazon firmasıyla başlayan bu trendi sonrasında Apple (iCloud), Google (App Engine, Google Docs) ve Microsoft (Azure) gibi bilişim firmaları ve birçok özel sektör kuruluşu hizmetleriyle devam ettirmiştir.

Bulut bilişimin özel sektör hizmetlerinde olduğu gibi kamu hizmetlerinin sunulmasında da faydalar sağlayacağı çok geçmeden anlaşılmış ve gelişmiş ve gelişmekte olan birçok ülke kamuda bulut bilişim mimarisinin kullanılması ve e-devlet uygulamalarının bulut üzerinden servis edilmesi konularında çalışmalara başlamışlardır. Gelişen teknolojiler ve çeşitlenen vatandaş talepleri sebebiyle; internet üzerinden statik, kamu odaklı, vatandaşın pasif kullanıcı olduğu e-devlet hizmetleri yerine; internet ve sosyal medya üzerinden platform bağımsız şekilde sunulan, vatandaş odaklı ve vatandaşların yönetim süreçlerine dâhil olabildikleri c-devlet hizmetlerinin gelişmeye başlaması, bu hizmetlerin sunumu için en uygun hizmet modeli olan bulut bilişim mimarilerinin kamusal alandaki önemini daha da artırmıştır.

Ülkemizde gerek Avrupa Birliği uyum süreci çerçevesinde ve gerekse de özel sektör kuruluşlarının iş ve işlemlerinde sağladığı maliyet, zaman ve personel tasarruflarını dikkate alarak; kamu kurum ve kuruluşları bilgi teknolojileri alanında proje ve yatırımlara hız vermişlerdir. Bu proje ve yatırımların hız kazanmasında bu dönemdeki hükümetlerin düzenleyici strateji ve eylem planlarının etkisi büyüktür. Bu bağlamda Avrupa Birliği tarafından başlatılan e-Europe+ girişimine paralel olarak 2002 yılında ortaya konulan e-Türkiye Girişimi Eylem Planı öncü nitelik taşımaktadır. Yine bu girişimin devamında e-Dönüşüm Türkiye Projesi başlatılmıştır. Bu projenin yürütülmesini sağlamak amacıyla 2003 yılında Kısa Dönem Eylem Planı ve 2005 yılında Eylem Planı hazırlanmıştır. 2005 Eylem Planının uygulanması sonrasında 2005-2006 yıllarında Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanarak 2006-2010 döneminde uygulanmıştır. Yine 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Kalkınma Bakanlığı Bilgi Toplumu Dairesi tarafından hazırlanmış ve bu eylem planında bulut bilişim teknolojileri ile ilgili fayda, tehdit, risk ve ayrıca kamusal hedeflere sıkça yer verilmiştir. Ayrıca 2013 yılında, Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 25. Toplantısında alınan 2013/104 sayılı karar uyarınca, kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir. Bu sayede yedeklilik, felaket kurtarma merkezi, siber güvenlik, iş sürekliliği, kamu bulutu, işletme maliyeti, kurumlar arası veri paylaşımı gibi hususların tamamına çözüm sağlanması amaçlanmıştır. Bu karar Türkiye'de bulut bilişim alanındaki çalışmalara ivme kazandıran bir nitelik taşımaktadır.

Uluslararası İş Yazılımları Birliği (Business Software Alliance – BSA) tarafından 2016 yılında yayımlanan ve dünya genelinde 24 ülkenin bulut bilişime hazırlık durumu hakkında yapılan incelemelere dayanan 2016 BSA Global Bulut Bilişim Puan Çizelgesi adlı çalışmada ülkemiz 19. sırada gösterilmiştir (BSA, 2016).

Ülkemizin gelişen bilişim teknolojilerine uyum sağlamaktaki kararlılığı ve bu doğrultuda yaptığı çalışmalar neticesinde, birçok kamu kuruluşu günümüz bilişim dünyasının gözdesi haline gelen bulut bilişim konusunda projeler geliştirmiş ve

geliştirmeye devam etmektedir. Bu doğrultuda, Bakanlığımızca yürütülen CBS Altyapısının Kurulması ve Geliştirilmesi projesiyle; Bakanlığımızın sahip olduğu bilişim kaynaklarının tek bir altyapıda toplanarak esnek, erişilebilir ve kullanılabilir şekilde iç ve dış kullanıcılara hizmet vermesinin sağlanması, gerek e-devlet uygulamalarımızın ve gerekse vatandaşlarımıza ve ihtiyaç duyan kuruluşlara hizmet veren diğer uygulamalarımızın bu altyapı ile platformdan bağımsız olarak güvenli şekilde sunulabilmesi ve uzun vadede kurulacak Kamu Entegre Veri Merkezi altyapısıyla entegrasyonun kolayca sağlanması amaçlanmıştır.

Günümüzde e-devlet konusunda öncü bazı ülkeler, geleneksel mimariye uygun şekilde geliştirilmiş uygulamalarını bulut bilişim mimarisine taşımakta zorluklar yaşamakta ve bu durum, ilgili ülkelerin bulut bilişime geçişlerini olumsuz yönde etkileyerek, kamu sektörlerinin bulut bilişim alanında göreceli olarak geri kalmalarına sebebiyet vermektedir. Bu sebeple, özellikle e-devlet hizmetleri açısından bakıldığında, gelecekte bulut bilişim altyapısında çalışacak ilgili hizmetlerin, geleneksel bilişim mimarilerine uygun şekilde kurulup yaygınlaşmasından önce, kamu altyapısının bulut mimarisine uygun hale getirilerek; geliştirilecek projelerin bu altyapıya uygun şekilde geliştirilmesi gerekmektedir. Bu şekilde ileride atıl duruma düşecek birçok yazılım ile ilgili kamu kaynağı israfının da önüne geçilmiş olacaktır.

Bulut bilişim, taşıdığı fayda ve avantajların yanında birçok riski de beraberinde getirmektedir. Bu risklerin bazıları hali hazırda kullanılan geleneksel bilişim mimarileri ile ortak riskler olsa da, bulut bilişimin kendine has riskleri de mevcuttur. Bu riskler; hizmet devamlılığı ve kullanılabilirliği, hizmet sağlayıcı bağımlılığı, veri güvenliği ve gizliliği, veri denetlenebilirliği, uygunluğu ve yasal düzenlemeler, ağ ve bant genişliği, yönetim ara yüzü, veri transferi, sağlayıcı alt yüklenicileri ve lisanslama vb. konularda bulut mimarilerinin maruz kaldığı tehdit ve zafiyetlerin sonucu olarak ortaya çıkan risklerdir. Bu risk konuları ilk bakışta karşımıza çıkan temel konular olup geleneksel bilişim mimarilerinin getirdiği riskler de eklenince; bulut bilişim kullanıcıları onlarca istenmeyen, bir kısmı öngörülemeyen ve hizmet kalitesini ve sürekliliğini tehdit eden riskle karşı karşıya kalabilmektedir. Bu sebeple bilişim sektörü için yeni sayılabilecek

bir mimari ve servis sağlama platformu olan bulut bilişim konusunda, kurum ve kuruluşların karşılaşabilecekleri ilgili risklere dair bir risk yönetim süreci oluşturmaları önem arz etmektedir.

Bu doğrultuda, günümüzde birçok kamu kurum ve kuruluşu bilişim teknolojileri alanında ilgi odağı haline gelen bulut bilişim ile ilgili olarak, karşılaşabilecekleri riskleri belirleyen, analiz eden, değerlendiren bir risk yönetimi modeline ihtiyaç duymaktadırlar. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), Bulut Güvenliği Ajansı (CSA), Microsoft, ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) vb. kuruluşların bulut bilişim mimarilerinde karşılaşılabilecek riskleri belirleme ve derecelendirme üzerine çalışmaları bulunmakla birlikte; yapılan araştırmalarda akademik literatürde bulut bilişim ile ilgili riskleri işleyip bir risk yönetim modeli oluşturan detaylı bir çalışmaya rastlanmamıştır. Bu tez çalışmasıyla; bulut bilişim alanında stratejiler belirleyen, bireysel yatırımlar yapan ve kurulacak Kamu Entegre Veri Merkezi ile gelecekte bilişim kaynaklarını tek veya yedekli birkaç merkeze entegre edecek olan kamu kurum ve kuruluşlarına; bulut bilişim risk yönetimi konusunda ışık tutmak; hizmetlerini internet üzerinden müşterilerine sunma, bilişim kaynaklarının kullanımı ve yönetimi ile ilgili verimliliği artırma gibi konularda referans alabilecekleri bir kaynak sunmak ve eksikliklerini gidermek amaçlanmaktadır.

Bu amaçla bu çalışmada, öncelikle bulut bilişimin ve bulut bilişimle yakından ilgili olan kavramların tanımına yer verilmekte ve sonrasında bulut bilişimin tarihçesi ve bir hizmet modeli olarak, geleneksel sunucu mimarilerinden bulut bilişime geçişi sağlayan ve zorunlu kılan faktörler karşılaştırmalı analiz metoduyla açıklanmaktadır. Ardından bulut bilişim servis modelleri, mimari çeşitleri, donanım ve yazılım katmanları ve kullanım metotları kısaca ele alınmakta ve ilk bölümün sonunda bulut bilişimin güçlü ve zayıf yönleri ile bulut bilişimle ortaya çıkan fırsat ve tehditler SWOT analiziyle ortaya konmaktadır. Bölümün genelinde, bulut bilişim kavramının açıklaması ve ilerleyen bölümlerde ele alınacak konulara ışık tutacak şekilde bulut bilişimle ilgili bir ön durum analizi yapılmaktadır.

Sonraki bölümde kurulması planlanan Kamu Entegre Veri Merkezi sürecine ilişkin hem altyapı, hem de hizmet ve uygulamalar bazında yapılması gerekenlerle ilgili açıklamalara ve örnek durum analizlerine yer verilmektedir. Öncelikle ülkemizin ve bulut bilişim konusunda öncü dünya ülkelerinin bulut bilişim alanında stratejileri, projeleri, faaliyet ve uygulamalarına yer verilmekte ve kamuda bulut bilişimin kullanımı ile ilgili örnek durumlar analiz edilmektedir. Sonrasında sırasıyla entegre kamu hizmetleri için gereksinimler, bulut bilişimin entegre kamu hizmetlerinin sağlanmasındaki önemi, kamu bulutu işletme modelleri, e-devlet uygulamalarının buluta aktarılması ve güvenlik, maliyet, iş sürekliliği ve kişi mahremiyeti konularında bulut bilişimin faydaları ve ortaya çıkan sorunlara yer verilmektedir. İlgili bölümde son olarak kamuda bulut bilişim kullanımı ile ilgili modellere ve çözüm önerilerine yer verilmektedir. Bu sayede, Türkiye ve dünyada bulut bilişimin mevcut durumu incelenerek; kamuda daha etkin kullanımının sağlanması ve geleceği ile ilgili gereksinim, politika ve stratejiler ortaya konmaktadır.

Bir sonraki bölümde; TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27005 Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Risk Yönetimi ve TS ISO 31000 Risk Yönetimi Standartları çerçevesinde risk ve ilgili kavramların kısa açıklamalarına yer verildikten sonra, sırasıyla bulut bilişimle ilgili varlıklar, tehditler, zafiyetler ve son olarak riskler belirlenmekte ve belirlenen bu riskler ile ilgili olasılık değerlendirilmesi, etki analizi ve risk değerinin bulunması yöntemleri uygulanarak ilgili riskler analiz edilmektedir. Böylece risk yönetimi modeli oluşturularak risklerin işlenmesi ve değerlendirilmesi için gerekli altyapı oluşturulmaktadır.

Son bölümde analiz edilen ilgili riskler yukarıda belirtilen standartlar çerçevesinde, risk işleme yöntemleri olan; risk kabul etme, transfer etme, azaltma ve kaçınma hususlarında değerlendirilmektedir. Yapılan değerlendirmeler sonrasında risklerin etkilerinin ve olasılıklarının azaltılması için gerekli önlem ve kontroller belirlenmekte, kabul edilebilir olanlar, kaçınılması gerekenler ve sözleşme veya sigortalama yoluyla dış kuruluşlara transfer edilebilecekler sebepleriyle ortaya konulmaktadır. Bu bölümde son olarak bulut risklerinin işlenmesiyle ilgili maliyet

analizi yapılmakta, risklerin periyodik olarak izlenmesi ve değerlendirilmesi için gerekli prosedürler ortaya konulmakta ve risklerin profilleri oluşturularak her bir risk için yapılan risk işleme prosedürleri özetlenmektedir.

Bu çalışmada genel olarak bulut bilişim teknolojisinin özellikleri ve kabiliyetleri incelenmekte, bu özellik ve kabiliyetlerin kamu kuruluşlarına yansıması ve kullanım sonrası ortaya çıkabilecek riskler analiz edilmektedir. Bu sebeple muhtelif bölümlerde, tüm olası risklerin analiz edilebilmesi adına, bulut bilişim mimarilerini kullanan ilgili kamu kurum ve kuruluşlarının; gerek özel sektör bulut sağlayıcılarının ve gerekse de kamu bulutu veya entegre veri merkezi kurmak ve işletmekle yükümlü bir kamu ajansının/kurumunun veya BİT sağlayıcısının müşterisi olması varsayımlarına yer verilmektedir. Yine olası tüm risklerin ve etkilerinin ortaya konulabilmesi adına bulut mimarisi kullanan ilgili müşteri kuruluşların kendi iç operasyonları ile birlikte, bu mimariler üzerinden vatandaşlara uygulama ve hizmetler sunmaları durumu göz önüne alınmıştır. Karşı karşıya kalınan ve tüm paydaşları (sağlayıcıyı, müşteri kuruluşu ve müşteri kuruluşun sunduğu hizmetleri kullanan vatandaşları) bir şekilde etkileyen bulut bilişim riskleri, ilgili müşteri kuruluş açısından ele alınmaktadır.

1. BULUT BİLİŞİMİN TEMELLERİ

1.1. Bulut Bilişim Nedir?

İngilizce “cloud computing” teriminin dilimize tercümesi olan bulut bilişimle ilgili onlarca tanım bulunmaktadır. Diğer birçok teknolojide olduğu gibi bulut bilişimin de kullanıcı ve sağlayıcı ihtiyaçları doğrultusunda gelişimini ve değişimini sürekli sürdürmesi, bulut bilişim teknolojisinin birçok bilişim teknolojisi alt bileşenini bünyesinde barındırması ve bulut bilişim kavramının ortaya çıkmasından önce hâlihazırda söz konusu alt bileşenleri kullanan ve sunan kuruluşların ortaya çıkan bu yeni kavramı kendi amaç ve hedefleri doğrultusunda tanımlamaları birçok farklı tanımın ortaya çıkmasına neden olmuştur. Bulut bilişimin ne olduğunu ve hangi amaca hizmet etmek üzere geliştirildiğini tam olarak anlayabilmek için bu kavramın ortaya çıkmasına katkıda bulunan teknoloji ve kabiliyetlerin tarihsel olarak gelişimine aşina olmak gerekmektedir. Bu noktada bulut bilişimin bünyesinde barındırdığı veya hizmet sağlamada faydalandığı platform bağımsız yaygın ağ erişimi, esneklik, ölçülebilirlik, talep üzerine self servis ve kaynak havuzu oluşturma gibi kabiliyetlerinin yanı sıra; sanallaştırma, çoklu kiracılık, servis odaklı mimari, istemci-sunucu modeli, API, dağıtımlı hesaplama ve Web 2.0 gibi bulut bilişimin etkinliğini artıran benzer teknoloji ve kavramların irdelenmesi önem taşımaktadır.

Bulut bilişimle ilgili genel kabul gören tanımlardan bir tanesi, bulut bilişimle ilgili birçok standardı belirleyen kuruluş olan NIST (ABD Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından yapılan tanım olup şu şekildedir; "Bulut bilişim, düşük yönetim çabası veya servis sağlayıcı etkileşimiyle, hızlı alınıp salıverilebilen ayarlanabilir bilişim kaynaklarının paylaşılır havuzuna, istendiğinde ve uygun bir şekilde ağ erişimi sağlayan bir modeldir" (Mell and Grance, 2011). Tanımdan da hareketle bulut bilişim, depolama ve veri işleme yükünü istemci bilgisayarlar üzerinden alıp, uzak sunucular üzerine aktaran bir hizmet modelidir. Sunucular üzerinde depolanan ve istemciler tarafından talep edilen işleme tabi tutulan veriler, ihtiyaç duyulduğu anda,

internet üzerinden istemci bilgisayarlara aktarılır. Verilere, platform bağımsız olarak farklı lokasyonlardan internete bağlı herhangi bir istemci cihaz üzerinden erişilebilir.

Şekil 1: Bulut Bilişimde Platform Bağımsız Erişim (Kaynak: Softaculous, 2015)

1.2. Bulut Bilişim İle İlgili Temel Kavramlar

Bu bölümde bulut bilişimin temel özelliklerinin yanı sıra bulut bilişimin etkinliğini artıran benzer teknoloji ve kavramlara değinilecektir.

1.2.1. Bulut bilişimin temel özellikleri:

Bulut bilişim teknolojisinin NIST tarafından ortaya konan tanımı beş adet temel özelliğe dayanmaktadır (Mell and Grance, 2011). Bunlar sırasıyla;

Talep üzerine self servis: Bir kullanıcının servis sağlayıcısı ile irtibata geçmeden sunucu kullanım süresi ve ağ depolama kapasitesi gibi bilişim kaynaklarını otomatik olarak ihtiyacı uyarınca temin edebilmesidir. Burada kullanıcı bilişim kaynaklarını elde etmek amacıyla herhangi bir onay talep etmeksizin, kendi belirlediği ihtiyacına göre kaynakları seçerek temin edebilmektedir. Başta uygulama geliştiriciler olmak üzere kullanıcıların isteğe bağlı olarak kaynaklarını temin edip, kullanabilmeleri onlara sınırsız bir kaynak havuzu içerisinde işlem yaptıkları hissini vermektedir. UC Berkeley RAD

Lab (Reliable Adaptive Distributed Systems Laboratory) hazırladığı bir raporunda, bulut bilişimin "sınırsız kaynak ilizyonu" yarattığını belirtmiş ve böylece bulut bilişim ortamındaki algının, BT kaynaklarının pahalı ve sınırlı olduğuna dair geleneksel algıdan ne kadar farklı olduğunu göstermiştir (Carstensen, 2012).

Platform bağımsız yaygın ağ erişimi: Bulut bilişim teknolojisinin kabiliyetlerinin, standart mekanizmalar aracılığıyla, ağ üzerinden erişilebilir ve kullanılabilir olarak çeşitli istemci platformları (örneğin cep telefonları, tabletler, dizüstü bilgisayarlar ve iş istasyonları) üzerinden sunulmasıdır. Erişim sağlayacak cihaz türünü sınırlamak için tasarlanmış özel protokoller veya lisans ihtiyacına göre belirlenen ücret veya telif ödemeleri yerine, bulut bilişim ortamında bağlantı ve iletişimi sağlayan HTTP gibi ortak protokoller kullanılmakta olup; kullanılan protokolü sağlayan cihazlar üzerinden erişim sağlanabilir. Ayrıca kullanılan ortak ağ protokolleri sayesinde kullanıcıların haricinde, çeşitli program ve API'lerin de bulut altyapısına erişimi mümkün olmaktadır. Ancak bu durum, ilgili program veya API'lerin kullanım durumuna göre veri trafiğinin ciddi biçimde artmasına neden olabilecek olup, bulut sağlayıcısının kaynak planlamasını zorlaştırmaktadır.

Kaynak havuzu oluşturma: Bulut sağlayıcısının farklı fiziksel ve sanal kaynaklarının birden çok tüketiciye hizmet etmek üzere bir araya getirilerek, dinamik müşteri talebine göre çoklu kiracılık modeli kullanılarak her bir müşteriye atanması, geri alınabilmesi ve tekrar atanabilmesidir. Bu yöntemde, sağlayıcı farklı lokasyonlardaki kaynaklarını bilişim kaynak havuzuna dâhil edebilmektedir. Bu durum müşterilerde, veri ve işlemlerinin tutulduğu lokasyonlar hakkında bir bilgisi ya da kontrolü olmadığı hissini yaratsa da, yüksek bir veri soyutlamasıyla verinin; veri merkezi, şehir ve ülke bazında nerede tutulduğu bilgisi sağlanabilmektedir (Carstensen, 2012). Geleneksel mimarilerde her bir iş için, o işin sunucuya getireceği maksimum yük hesaplanarak sunucular tahsis edilirken; bulut bilişimde o anda kullanılan uygulamaların verimli çalışabilmesi için gereksinim duyulan kaynak ihtiyacına göre kaynaklar atanır ve gereksinim sona

erdiğinde geri alınabilir. Böylece yılın belli dönemlerinde kullandığı yük miktarı normalin çok üzerine çıkan uygulamaların kesintisiz hizmet vermesi sağlanmış olur.

Birçok farklı görev ve hizmeti yerine getirmek için kurulmuş kamu kurum ve kuruluşlarının sağladıkları hizmetler düşünüldüğünde, bazı hizmet ve görevlerin yoğunluğunun özellikle yılın belli dönemlerinde artış gösterdiği, yılın kalan bölümlerinde ise göreceli olarak düşük yoğunlukta seyrettiği görülecektir. Örneğin, kurumların finans ve mali hizmetler ile ilgili bölümlerinin iş yükünün ve kullandıkları ve servis ettikleri uygulamalara ait veri trafiğinin yılın son çeyreğinde veya maaş ödeme günlerinde katlandığı; aynı şekilde vergi tahsilatı yapan birimlerin iş ve servis ettikleri uygulamalara ait yoğunluklarının, vergi ödemelerinin son günlerinde büyük bir artış gösterdiği bilinmektedir. İlgili kurumlar bu noktada bulut bilişim mimarisi yardımıyla söz konusu yoğun günlerde edindikleri tecrübeye dayalı olarak diğer birimleri için yedek olarak ayırdıkları kaynaklarını (depolama alanı, işlemci gücü, bant genişliği), ilgili yoğun birimlere aktararak hem ilgili birim personelinin kullanımı için geliştirilmiş uygulamaların ve hem de dışarıya servis ettikleri uygulamaların kullanılabilirlik ve erişilebilirliğin sürdürülebilmesini sağlayabilirler. Bu sayede bu birimler için sadece yılın belli dönemlerinde pik yapan hizmetlerinde kullanılmak üzere ek fiziksel bilişim kaynağı temini ihtiyacı ortadan kalkmış olur.

Esneklik: Bulut müşterilerinin ihtiyacına göre, talepleri doğrultusunda anlık olarak kullandıkları kaynak kapasitesinde genişleme ve daralma sağlanabilmesidir. Kapasite esnek bir şekilde artırılabilir veya artırılan kapasite hızlı bir şekilde iade edilebilir. Bu sayede kurum ve kuruluşlar iş kapasitelerine göre kaynak miktarını hızlıca ayarlayabilir ve iş verimlerini kısa sürede artırabilirler. İhtiyaç halinde dakikalar içinde yapılabilecek kaynak artışı ile uygulamalarını uygun hizmet seviyelerinde tutup, kullanıcı memnuniyetini artırabilirler. Bulut bilişimde esneklik özelliği, birçok durumda insan faktörünü de ortadan kaldırarak, bulut mimarisindeki uygulamaların kendi performans seviyelerini takip edip, düzgün ve efektif çalışabilmeleri için ihtiyaç duydukları anda bilişim kaynaklarını otomatik olarak talep edip, temin edebilmelerine imkân tanımaktadır. Dakikalar içerisinde sağlanan bu altyapı iyileştirilmesi, uygulama

gruplarının anlık yükselen kullanım durumuna ve iş yüküne kısa sürede cevap vermesini sağlayarak iş verimliliğini artırır.

Bulut müşterisinin kullandığı bilişim kaynağını hiçbir ek taahhüt ve sorumluluk olmaksızın artırıp azaltabilmesi doğal olarak bulut sağlayıcısı için kapasite planlaması ve kaynak kullanım riskini ortaya çıkarabilmektedir. Ayrıca bulut müşterisi için teoride sınırsız bir kaynak havuzu ilizyonu yaratıyor gibi görünen altyapı, pratikte sınırsız değildir ve bütün bulut sağlayıcıların kategorilere göre kaynak kiralama limitleri mevcuttur. Bu sebeple kaynaklarını müşterilerine kiralayan bulut sağlayıcılarının, gerekli alt yapı maliyetlerini göz önünde tutarak zarar uğramamaları için, müşterilerinin dönem dönem dalgalanan kaynak kullanım miktarlarını çok iyi ölçerek bu doğrultuda gerekli kapasite planlaması optimizasyonunu yapmaları ve farklı müşterilerle yapacakları kullanıma esas hizmet seviye anlaşmalarını (SLA) bu doğrultuda hazırlamaları gerekmektedir.

Ölçülebilirlik: Bulut mimari altyapısı, sağlayıcıların hizmet türüne göre (depolama kapasitesi, işlemci kullanımı, bant genişliği ve aktif kullanıcı hesapları) otomatik olarak kaynak kullanımını kontrol ve optimize etmeleri için ölçüm yapma imkânı tanır. Bu doğrultuda kaynakların kullanım miktarları hem müşteri hem de sağlayıcı tarafından izlenebilir, kontrol edilebilir ve arşivlenebilir. Kullanıcıların ihtiyaç duydukları kaynakları, hizmet seviye anlaşması (SLA) haricinde hiçbir ek taahhüt ve sorumluluk yüklenmeden, esnek bir şekilde, kısa bir sürede ve sınırsız erişim sağladıkları bir kaynak havuzundan self servis şeklinde temin ettikleri bulut mimarisinde; kullanılan kaynakların ücretlendirilebilmesi için ölçülebilirliği son derece önemli ve kritik hale gelmiştir. Ayrıca bulut müşterilerinin uygulamalarının değişen yük ve veri trafiği ihtiyaçlarına göre kullanım miktarlarını ölçüp arşivleyebilmesi, servis ettiği uygulamalarının kullanım durumuna göre hangi miktarda kaynağa ihtiyacı olduğunu, sahip olduğu arşivden hesaplayabilmesine ve edindiği tecrübe doğrultusunda kiraladığı bilişim kaynağını artırıp azaltabilmesine olanak sağlamaktadır. Böylece bulut müşterisi optimum uygulama tepki sürelerini koruyacak şekilde, ihtiyacından fazla kaynağa sahip olduğunu fark ettiğinde bu kaynağı geri vererek kiralama maliyetinden tasarruf sağlayacak,

uygulamaya aşırı yüklenme olduğu durumlarda da kaynağı hızlı bir şekilde artırarak, uygulamanın kullanılabilirliğini ve erişilebilirliğini muhafaza edebilecektir.

Burada bulut servis sağlayıcısının kaynaklarını kiralayan bulut müşterisinin kullandığı hizmet ile ilgili olarak ne şekilde ödeme yapacağı ilk etapta bir sorun haline gelebilir. Geleneksel mimaride kurum veya kuruluşlar kullandıkları bilişim kaynakları için yaptıkları sözleşmeler uyarınca dönemlik sabit ücretler öderken, kullandığın kadar öde prensibine göre yapılacak ödemeler için farklı finansal muhasebe yöntemi tasarlamaları gerekecektir. Ayrıca birçok kuruluş farklı bilişim ihtiyaçları için farklı birimleri aracılığıyla alım ve ödeme yapmaktadırlar. Bu sorunların çözümü için öncelikle tüm BT kaynaklarına ait ücretlerin tek bir finansal yapı tarafından yönetilmesi, ücretlendirmenin yapılacak hizmet kullanım anlaşması ile birim kullanım miktarlarına göre birim fiyatlar belirlenerek standart hale getirilmesi ve uzun vadede servis edilecek uygulamaların, insan faktörünü ortadan kaldırarak, kendi yük durumlarına göre ihtiyaç duydukları anlık BT kaynağını otomatik olarak artırıp azaltmayı talep edip temin edebilecekleri şekilde tasarlanmaları ve işletilmeleri gerekecektir.

1.2.2. Bulut bilişim benzeri teknoloji ve kavramlar

Yukarıda da bahsedildiği üzere, bulut bilişim mimarisinin kabiliyetlerinin ve getirdiği yeniliklerin daha iyi anlaşılabilmesi için; bulut bilişim öncesinde kullanılan geleneksel BT mimarisinden, bulut bilişime geçiş sürecinde önem taşıyan ve bir kısmı hali hazırda bulutun bir alt bileşeni olarak kullanılıp, etkinliğini artıran önemli bazı bulut bilişim benzeri teknoloji ve kavramlar şu şekildedir:

Sanallaştırma: Sanallaştırma, bulut bilişimin gelişmesini teşvik eden temel bir teknoloji platformudur ve bu platform modern veri merkezlerinin çehresini değiştirmektedir. Sanallaştırma terimi bilişim kaynaklarının (CPU, depolama, ağ, bellek, uygulama yığını ve veritabanı) hizmet tüketen uygulamalar ve son kullanıcılardan soyutlanması anlamına gelir. Altyapı soyutlaması, ister altyapı isterse de uygulama ve veri olsun havuzda toplanan tüm kaynakların, standart yöntemlerle onları kullanmak için yetki verilen herhangi bir kişi veya program tarafından kullanılabilir ve erişilebilir olmasını sağlar.

Sanallaştırma teknolojileri, tüm kiracılar için ölçeklenebilir ve paylaşılan bir kaynak platformu sağlayarak; çok kiracılı bulut iş modellerine olanak sağlar. Daha da önemlisi, platform tüketicileri için özel bir kaynak görünümü sağlar. Bir kuruluş açısından bakıldığında sanallaştırma, veri merkezi konsolidasyonu sunarak ve BT'nin operasyonel verimliliğini artırmaktadır (Mather, 2012).

Sanallaştırma teknikleri ağlar, depolama üniteleri, sunucu donanımı, işletim sistemleri, uygulamalar ve diğer BT altyapı katmanlarına uygulanabilir. Sanallaştırma teknolojileri bilgisayar, depolama, ağ donanımı ve üzerinde çalışan uygulamalar arasında bir soyutlama katmanı sağlar. Bu soyutlama katmanı tek bir fiziksel makineye birden fazla sistemin özelliğini aktarmak için kullanılır. Kurulan bu sistemler ayrı karakteristik özelliklere (Windows, Linux, MacOS vb) sahip olabilir. Her fiziksel makine üzerinde çalışan her bir sanal işletim sistemi, yürütmekte olduğu işle ilgili olarak bağımsız olarak programlanabilmekte ve diğer sanal işletim sistemleri bu işlemlerden etkilenmemektedir.

Sanallaştırma platformunun başta BT maliyetlerini azaltmak olmak üzere kurum ve kuruluşlara sağladığı birçok avantajlar vardır. Örneğin sunucu sanallaştırması kullanılarak fiziksel sunucu sayısını azaltılabilir ve böylece bakım, barınma, enerji ve güvenlik maliyetlerinde tasarruf sağlanabilir. Ayrıca kullanılmakta olan mevcut donanımın yapılan işin gereklerini yerine getirmediği durumlarda, yenisini almak yerine sahip olunan sanal donanımın özelliklerini artırma kabiliyeti kazandırmaktadır. Yine veri kurtarmaya yönelik yedekleme sistemleri daha fazla donanım teminine gerek kalmadan kolayca kurulabilmekte ve verimli bir şekilde kullanılabilmektedir. Sanallaştırma sayesinde ister yerelde isterse bulutta olsun, veri yığınları aktarımı ve program yüklemeleri mevcut sunucudan yeni donanımlara çok daha hızlı bir şekilde yapılabilir. Böylece her yeni donanım için ayrıca sistem kurulumu süresi en aza indirgenebilir.

Sanallaştırma ve bulut bilişim birbiriyle sıkı şekilde ilişkili olan ve bilişim kaynaklarından en iyi şekilde yararlanarak altyapı maliyetlerini azaltmak için uygulamaya alınan yöntemlerdir. Her iki yöntemde de donanım katmanları uygulama

katmanından soyutlanmakta, fiziksel bilişim kaynaklarından ihtiyaca göre sanal kaynaklar yaratılmakta ve bu sanal kaynakların miktarı ihtiyaca göre değiştirilebilmektedir. Bulut bilişim, kurumsal hizmet ya da uygulamaların dağıtılmış bilgisayarlardan oluşan bir ağda çalıştırılmasına olanak tanır. Sanallaştırmanın getirdiği teknolojik yeniliklere ek olarak bulut bilişimde; bilişim kaynaklarının bulut sağlayıcısına bağlı kalmaksızın artırılıp azaltılabilmesi, kullanılan kaynak miktarının anlık ölçülüp takip edilebilmesi ve aynı fiziksel makine üzerindeki kaynakları kullanan farklı müşterilerin yapılan ölçümler baz alınarak ücretlendirilebilmesi vb. sağlanabilmektedir. Özetle sanallaştırma, bulut bilişim tarafından kullanılan ve bulut bilişimin gelişiminde bir kilometre taşı vazifesi gören bir platformdur.

Çoklu Kiracılık (Multitenancy): Çoklu kiracılık, bir uygulama örneğini birden fazla kiracı arasında paylaşmak için, uygulama üzerinde her kiracıya adanmış özel bir "pay" sağlayan, performans ve veri gizliliği açısından diğer paydaşların izole edildiği bir yaklaşımdır. Burada, çoklu kiracılığın yanı sıra, kiracı alanı kavramı da karşımıza çıkmaktadır. Bir kiracı alanı, müşterilerin önceden tanımlanmış miktarda kaynakları kiraladığı ve bu alanlarda farklı uygulama örneklerini çalıştırabildiği kaynak alanlarını ifade eder (Krebs, 2012).

Bilişim kaynaklarının tek bir kullanıcı veya sahibine adandığı önceki bilişim modellerinin aksine bulut bilişim; kaynakların ağ, barındırma ve uygulama düzeyinde paylaşıldığı (birden çok kullanıcının aynı kaynağı kullandığı) bir iş modeline dayanmaktadır (Mather, 2012).

Tanımlardan da anlaşılacağı üzere çoklu kiracılık, bir veya birden çok sayıda ve türde bilişim kaynağının ihtiyacı olan farklı kullanıcılara, kullandığın kadar öde prensibi uyarınca kiralanmasıdır. Bu teknolojinin başlıca faydalarını:

- Kullanılabilecek azami yük kapasitesinin artırılması,
- Altyapının merkezileştirilmesi ve maliyetlerin düşürülmesi,
- Büyük oranda atıl kalan sistemler için verimliliğin artırılması,
- CPU, depolama ve ağ bant genişliği kaynaklarının dinamik olarak ayrılması,

- Hizmet sağlayıcı tarafından izlenebilen istikrarlı performans, olarak sıralayabiliriz.

Çoklu kiracılık ile bulut bilişim arasındaki en önemli fark, bulut bilişimin tek bir ağ veya donanım üzerinde çalışmayıp, internet üzerinde bir havuzda toplanan farklı lokasyonlardaki kaynaklara bağlı olmasıdır. Oysa çok kiracılı ortamlarda birden fazla müşteri aynı veri depolama mekanizmasıyla, aynı donanım ve aynı işletim sistemi üzerinde çalışan, aynı uygulamayı paylaşmaktadır. Uygulama tasarımı ile müşteriler arasında oluşturulan bölümleme (segmentasyon) sayesinde, kullanıcılar birbirlerinin verilerini göremez. Dağıtık bir yapısı olan bulut bilişimde ise her bir müşteri için birbirinden bir veya birçok fiziksel makine üzerinde, kişiye özel sanal makineler oluşturulmuştur ve bu sayede her kullanıcı sanal da olsa birbirinden ayrılmıştır. Ayrıca bulut bilişimdeki esneklik özelliği sayesinde kullanıcıların ihtiyaçlarına göre kaynak kullanım miktarlarını değiştirebilmeleri avantajı çoklu kiracılık iş modelinde sağlanamaz. Bu sebeple, bulut bilişim mimarisinin çoklu kiracılık iş modelinden çok daha kapsamlı ve esnek olduğu açıkça ortaya çıkmaktadır.

Servis Odaklı Mimari: Servis odaklı mimari (Service-Oriented Architecture (SOA)), bilgisayar sistemlerinin işlevselliklerini, iş süreçleri etrafında gruplaştırarak sistem geliştirmesi ve bütünleştirilmesinde yol gösteren bir yazılım tasarımı felsefesidir. SOA altyapısı, iş süreçlerine katılan değişik yazılım uygulamalarının birbirleriyle haberleşmek üzere yazılmamış olmalarına rağmen veri alışverişinde bulunmalarını sağlar. Servis odaklılık, hizmetlerin işletim sistemleri, programlama dilleri ve diğer teknolojik ayrıntılarla ancak gevşek bir bağ oluşturmasını hedeflemektedir (Newcomer, 2005).

SOA, ağ hizmetlerinin kurumsal uygulamalar tarafından çok sayıda müşteriye sorunsuz bir şekilde hizmet verebilecek şekilde geliştirilebilmeleri için gerekli politika, ilke ve çerçeveleri içerir. SOA, ayrıca sunulan hizmetlerin yeteneklerini artırmaya yönelik olarak bir dizi servis şeklinde sunulduğundan, birbirine bağlı iş hizmetlerinin oluşturulmasını teşvik eden bir mimari tarzı olarak nitelendirilebilir. Bir kurum veya kuruluş kendi görev veya faaliyet alanında olan bir hizmeti internet üzerinden

sunabilmek için diğer kurum ve kuruluşların servis ettiği verilere ihtiyaç duyabilmektedir. Örnek vermek gerekirse, e- devlet üzerinden vatandaşların tapu bilgilerini sunan bir kurum, vatandaşların nüfus bilgileri ve parsel bilgilerinin harita görüntülenebilmesi için altlık haritalar vb. servislerle haberleşmek ve onlardan veri almak zorundadır. İşte SOA, bu alışverişe imkân tanıyan teknoloji, ilke ve çerçevelerle ilgili standartları belirleyen, iş süreçleri için gelişmiş yönetim kontrolü, görünürlük, entegrasyon ve ölçümleri sağlayan ve problemler için karma çözümler sunan bir tasarım felsefesidir. Burada altyapıyı sağlayan bilişim kaynaklarında herhangi bir problem yaşandığında, sistem hemen yedek bilişim kaynaklarını devreye alarak birbiriyle bağlantılı servislerin sürekli hizmet vermesini temin etmeye çalışır.

SOA ve bulut bilişim birçok yönden ortak gibi görünse de temelde farklı iki kavramdır. SOA'da mevcut uygulamalardan diğer programlara web servisler sağlanırken; bulutta yazılım servisleri son kullanıcılar ve çalışan programlar için tedarik edilir. Yine yönetim katmanı SOA'da mimarinin temel bir katmanıyken, bulutta yönetimde kullanıcının da söz sahibi olması nedeniyle genellikle ihmal edilir. Bulut bilişimin SOA'ya göre diğer bir üstünlüğü ise esnek yapısı sayesinde genişlemeye müsait olması olup, SOA'da bu zorlu ve pahalı bir süreçtir (Rittinghouse, 2010).

İstemci-Sunucu Modeli: İstemci-sunucu modeli, sunucu adı verilen kaynak veya hizmetin sağlayıcıları ile istemci denilen hizmet talep edenler arasında görev veya iş yükünü paylaştıran dağıtılmış uygulama yapısıdır. Burada sunucular kendi bilişim kaynaklarını istemciler ile paylaşırken, istemciler herhangi bir kaynak paylaşmayıp sadece sunucudaki içeriği veya sunulan hizmet uygulamasını talep ederler. İstemciler kendilerinden gelen istekleri bekleyen sunucularla iletişim oturumları başlatırlar ve gerek duydukları verinin pek çoğunu ya da tamamını uygulama sunucusundan isterler. İstemci-sunucu modelinin en güzel örneği internettir. Burada bilgisayar ve onun üzerinde çalışan web tarayıcı istemci rolündeyken, sayfaya ait veri ve uygulamaları barındıran bilgisayarlar, uygulamalar ve veri tabanları sunucu olarak adlandırılır. İstemci bilgisayarların web tarayıcısı aracılığıyla talep ettiği veri veya hizmetleri, sunucu

bilgisayarlar toplayarak, yine web sitesi görüntüsünde cevaplandırır ve istemcinin kullanımına sunarlar.

2000'li yıllarda web uygulamaları, belirli bir mikro mimari için geliştirilen rakip uygulama yazılımları kadar olgunlaşmıştır. Bu olgunlaşma, daha uygun yığın depolama ve servis odaklı mimarilerin gelişimi, 2010'lu yıllarda bulut bilişim trendini doğuran etkenler arasındadır (Barros, 2006).

Uygulama Programlama Arayüzü (API): API'ler (Application Programming Interface) adından da anlaşılacağı üzere kullanıcılara geliştirecekleri yazılım veya uygulama ile ilgili olarak gerekli program bloklarını, protokolleri, rutinleri ve araçları sunan programlardır. Bir API; web tabanlı bir sistem, işletim sistemi veya veritabanı sistemi için olabilir ve verilen bir programlama dilini kullanarak o sistem için uygulama geliştirmeye yönelik olanaklar sağlar.

İlgili bulut bilişim hizmetine uygun bir API, bulut bilişim hizmet modelinin uygulanmasını kolaylaştıran bir faktördür. API'ler, kaynakların self servis olarak müşteriler tarafından temin edilmesi ve programlarla kontrolü gibi konuları etkinleştirerek bulut bilişimi güçlendirirler. Bulut hizmeti dağıtım modeli (SPI) türüne bağlı olarak, API'ler gelişmiş SOA benzeri programlama modellerinden, basit URL manipülasyonlarına kadar farklı şekillerde tezahür edebilir. API'ler de bulut bilişim tam olarak potansiyelini kullanmasına yardımcı olurlar ve mevcut BT yönetim süreçleri ve hizmetlerinin bulut uygulamalarına yansıyan karmaşıklıklarını maskelerler. Örneğin, Amazon EC2, Sun Cloud, ve GoGrid gibi bulut servis sağlayıcıları tarafından sunulan API'ler, kullanıcıların işlemci, depolama ve ağ bileşenleri de dâhil olmak üzere bulut kaynaklarını oluşturmalarına ve yönetmelerine olanak vermektedir (Mather, 2009).

Günümüzde API bulut bilişim ilişkisindeki en önemli sorunlardan biri, her bulutun kendine özel benzersiz API'leri olması ve bu sebeple de, bulut uygulamalarının farklı bulutlar arasında aktarılabilir olamaması ve farklı bulut platformları üzerinde çalışan farklı uygulamalar arasında birlikte çalışabilirliği sağlamanın zor olmasıdır. Her API üzerinde çalıştığı bulutun hizmetine özgü olduğundan, uygulama geliştiriciler ve

veri merkezi personeli platforma özgü özelliklere aşina olmak zorunda kalmaktadır. Bu sorunun çözümüne yönelik, bütün bulutlar üzerinde çalışabilecek API'ler konusunda standartların ortaya konulması hususunda çeşitli çalışmalar halen devam etmektedir.

Dağıtımlı Hesaplama (Grid Computing): Dağıtımlı hesaplama, bilgisayar kaynaklarının (işlemci gücü, hafıza, depolama, yazılım, veri) esnek ve güvenli bir biçimde; kişi ve kuruluşlar tarafından internet üzerinden paylaşımı olarak tanımlanabilir. Burada amaç büyük miktarda veri üzerinde çalışma yapılması gereken hesaplamalar ve uygulamalar için daha fazla işlemci gücü kullanılarak işin kısa zamanda, güvenilir bir şekilde ve düşük bir maliyetle bitirilebilmesidir. Dünyanın farklı yerlerinde bulunan küme bilgisayarların, süper bilgisayarların veya kişisel bilgisayarların birbirine ağ ile bağlanması ile oluşturulmuş mekanizmadır. Her bir bilgisayar tekil olarak kendi payına düşen işlemi yapar ve merkezi bilgisayara çıkardığı işlem sonucunu gönderir. Bu sonuçlar merkezi bilgisayar tarafından harmanlanarak işlemin yapılması sağlanır.

Dağıtımlı hesaplama genellikle bulut bilişim ile karıştırılmaktadır. Birçok bulut bilişim servisleri bugün dağıtımlı hesaplama uygulamaları tarafından desteklenmektedir fakat bulut bilişim dağıtımlı hesaplamanın daha faydalı ve gelişmiş bir modeli ve bir sonraki adımı olarak görülmelidir (Rittinghouse, 2010). Zira sanallaştırma açısından bulut bilişim kadar gelişmemiş olan dağıtımlı hesaplama mimarisinde donanım arızası nedeniyle hizmet kesintisi olasılığı daha fazladır. Ayrıca entegre edilebilir dağıtık bilişim kaynağı sayısı bulut bilişimde daha fazla olduğundan, düşük kapasiteli çok sayıda sunucu ile altyapı kurulabilirken; dağıtımlı hesaplamada göreceli olarak daha büyük kapasiteli ve pahalı makinelere ihtiyaç duyulmaktadır.

Web 2.0: 2004 yılında gerçekleştirilen the O'Reilly Media Web 2.0 konferansında Tim O'Reilly ve Dale Dougherty tarafından ele alınan ve popüler hale getirilen Web 2.0 terimi, internet sitelerinin gelişen iletişim ve ağ teknolojileri sayesinde, kullanıcı tarafından içerik oluşturulması, kullanışlılık ve birlikte çalışabilirlik konularında gösterdiği gelişimi vurgulamaktadır.

Web 2.0 çerçevesinde geliştirilen bir web sitesi, pasif içerik görüntüleme ile sınırlı sitelerin aksine, sanal topluluk içinde kullanıcı tarafından içerik oluşturmasına imkân sağlayarak, kullanıcıların etkileşimine ve sosyal medya üzerinden diyalog yoluyla birbirleriyle işbirliğine izin verir. Web 2.0 örnekleri olarak; sosyal ağ siteleri, bloglar, wikiler, folksonomiler, video paylaşım siteleri, barındırılan servisler, web uygulamaları ve mashuplar verilebilir.

Bir Web 2.0 sitesini sadece okumak yerine herhangi bir kullanıcı, yayınlanan makaleler hakkında yorum yapmak veya sitede bir kullanıcı hesabı veya profil oluşturmak suretiyle sitenin içeriğine katkıda bulunmaya davet edilir. Bu durum, sitenin hali hazırda var olan yeteneklerini artırarak, kullanıcıyı; kullanıcı arayüzü, uygulama yazılımı ve dosya depolama üniteleri ile ilgili olarak kendi tarayıcısına daha fazla güvenme konusunda teşvik eder. Web 2.0'nin başlıca özelliklerine sosyal ağ siteleri, öz-yayın platformları, etiketleme, butonlar ve sosyal imleme dâhildir. Bu öğeler, kullanıcıları, kullandıkları uygulamaya değer katmak için teşvik eden birer "katılım mimarisi" olarak değerlendirilebilir (O'Reilly, 2005).

Web 2.0 ve bulut bilişim mimarilerinde sağlanan son gelişmeler, vatandaşların Web 2.0 yoluyla, mobil iletişim hizmetlerine ve kamu hizmetlerine e-katılımına katkıda bulunmaktadır. Burada kullanıcılara, kamusal alanlardaki bilgi akışı ile ilgili olarak daha fazla denetime sahip olma olanağı sunulmaktadır. Bu noktada bulut bilişim, Web 2.0 uygulamalarının aktarılarak vatandaşların e-katılımının sağlaması için bir platform olarak görülebilir (Mahmood, 2015).

1.3. Bulut Bilişimin Gelişimi ve Tarihçesi

Bulut bilişim terimi 90'ların ortalarına kadar internet için kullanılan bir benzetme olup, bulut sembolü de interneti temsil etmekteydi. Önceleri sadece servis sağlayıcı ve kullanıcı arasındaki ağ sistemini temsil eden bir telekomünikasyon kavramıyken, gelişen teknolojiyle birlikte bünyesine sunucu sistemlerini de ekleyerek tam bir bilişim terimi haline gelmiştir. Yine 90'lı yıllarda telekomünikasyon şirketlerinin özel sanal ağ hizmetleri vermeye başlaması ve bu ağların kullanımını kontrol altında tutmak için trafik

anahtarlama ve ağ bant genişliği teknolojilerini daha etkin kullanmaya başlamaları bir anlamda bugünkü manada bulut bilişimin temellerini atmış oldu.

John McCarthy'nin bulut bilişimle ilgili olarak 1960'larda, bilgi işlem kullanımının bir gün elektrik ve su hizmeti gibi bir kamu hizmeti şeklinde organize edilebileceği konusunda öngörüleri vardı. Yine bulut bilişimin günümüz özelliklerinin neredeyse tamamı (esnek hizmet sağlama, kamu hizmeti olarak sağlanma, çevrimiçi ağ üzerinde bulunma, sınırsız kaynak ilüzyonu) elektrik dağıtım sektörü ile kıyas edilerek ve genel, özel, kamu ve topluluklara ayrı kullanım formları düşünülerek; Douglas Parkhill'in 1966 tarihli "The Challange of Computer Utility" adlı kitabında incelenmişti. Bazı araştırmacılar ise bulut bilişimin tarihini 1950'lere, bilim adamı Herb Grosch'un bütün dünyanın aptal (dumb) terminaller üzerinden, 15 adet büyük veri merkezinde çalışan bir sistem kullanacağı varsayımına dayandırmaktadır (Ryan, 2011).

1950'lerde çeşitli kurum ve şirketlerde kullanılan ana çatı bilgisayarlar bulut bilişim alanında pek çok fikrin gelişmesine katkı sağlamıştır. Bu bilgisayarların tedarik edilmesi o yıllarda çok masraflı olduğundan; son derece pahalı olan bilişim kaynağının zaman paylaşımı (time sharing) olarak bilinen yöntemle, birçok kullanıcının ilgili bilgisayarı hem fiziksel erişimde hem de CPU kullanımında paylaşmasına izin veren, bilgisayarın boş kalma süresini en aza indiren bir sistem geliştirilmesi ihtiyacı doğmuştur. Zaman paylaşımı, bilgisayar işlemcisinin giriş/çıkış işlemlerini bekleyerek harcadığı zamanı diğer kullanıcılara tahsis etmesini ve bu sayede zamanın paylaşımlı ve verimli kullanımını öngörmüştür. Ortak veriler üzerinde çalışma ve hesaplama servislerine uzaktan erişim işlemleri, kısıtlı işlevdeki uç birimlerin telefon hattı üzerinden merkezi bir sunucuyla zaman paylaşımlı olarak bağlantı kurmaları şeklinde gerçekleşmiştir. Bu felsefe günümüzde kullanılan sanallaştırma ve bulut bilişim mimarilerinin de temelini oluşturmaktadır.

70'li yılların sonunda istemci-sunucu mimarisinin kullanılmaya başlaması bulut bilişimin gelişmesinde önemli bir dönüm noktasıdır. Yine bilgisayar ağlarının gelişmesi ve yaygınlaşmasıyla ortaya çıkan internet kavramı bulut bilişimin temel taşlarından

biridir. İnternetin ortaya çıkmasından çok yaygınlaşması bulut bilişimin doğuşunda büyük önem taşımaktadır. İnternetin yaygınlaşmasında, AHHP ve ICP gibi alt düzey protokol katmanlarının yerine, 80'li yıllarda daha esnek ve güçlü TCP/IP protokolünün kullanılmaya başlanmasının önemi büyüktür. Ayrıca 1993 yılında NCSA (National Center for Supercomputer Applications) tarafından geliştirilen Mosaic isimli internet tarayıcısı, Netscape firması tarafından 1994 yılında piyasaya sürülen Mozilla ve Microsoft firmasının 1995 yılında piyasaya sürdüğü Explorer internet tarayıcıları, internetin dünya çapında yaygınlaşmasını sağlayarak bir anlamda bulut teknolojilerinin önünü açmış ve gelişimine katkı sağlamışlardır.

1999 yılında Salesforce firmasının ilk kez bir kuruluşa ait uygulamayı internetten hizmete açması ve aynı yıl Google firmasının web tarayıcısının piyasaya sürülmesi gerek internetin ve gerekse de bulut mimarisinin kullanılabilirliğini artırmış ve önünü açmıştır. Yine 2002 yılında Web 2.0 kavramının ortaya çıkması ve bu felsefenin etkisiyle, kullanıcı tarafından oluşturulan ve dinamik ara yüzlere sahip web sayfalarının ortaya çıkmaya başlaması ve hemen ardından sosyal ağ sitelerinin gelişerek kullanıcıların verilerini hizmet sağlayıcılar tarafından kendilerine tahsis edilen sayfalarda paylaşabilmeleri, kullanıcıların bulut bilişim mantığına aşinalığını artırma konusunda önemli bir etki yaratmıştır.

2000'li yılların başında, yüksek kapasiteli ağların her yerde kullanılabilir olması, bilgisayarların ve depolama cihazlarının ucuzlamasının yanı sıra donanım sanallaştırmasının yaygın olarak benimsenmesi ve hizmet amaçlı mimari bulut bilişimde çok büyük bir büyümeye önayak oldu (Meulen, 2008).

Günümüzde kullanılan bulut bilişim felsefesinin temeli, Amazon firmasının veri merkezlerini modernize etmesiyle ortaya çıktı. Bu dönemde bilgisayar ağlarının çoğu kapasitelerinin %10'unu kullanıyordu ve sadece özel durumlardaki kapasite artışları için bütün sistem beklemekteydi. Amazon boş bekleyen bu kaynakları bilgi işlem servisi olarak kullandı. Yeni bulut mimarisinin temelinin atılmasının sonucu olarak önemli şirket içi verimlilik artışları yaşandı. Amazon'un küçük aktif çalışan ekipleri olan "iki

pizza takımları" vasıtasıyla yeni özellikler kolayca eklendi. Amazon şirket içinde geliştirdiği bu hizmetleri dışarıya pazarlamak üzere yeni ürün geliştirme çalışmalarını başlattı ve Amazon Web Hizmetleri (AWS) 2002 yılında hizmete girdi (Hof, 2006). Amazon Web Hizmetlerinin 2006 yılında hizmete aldığı Amazon S3 ise günümüzde kullanılan manada ilk gerçek bulut bilişim hizmeti olarak değerlendirilmektedir.

2007 yılında Apple firmasının herhangi bir kablosuz ağ üzerinden kullanılabilen İphone ürününü piyasaya sürmesi, bulut bilişimin mobil ortamda gelişimine önemli bir katkı sağlamıştır. 2008 yılında ise açık bulut (public cloud) kavramına ek olarak özel bulut kavramı doğmuş ve kuruşların kendi hizmetlerine özel daha güvenli bulut platformları oluşturmalarının önü açılmıştır.

Yine 2008'de Eucalyptus, özel bulutların yerleştirilmesi için kullanılan Amazon Web Servisi-API uyumlu ilk açık kaynaklı platform oldu. OpenNebula ise Avrupa Komisyonu tarafından desteklenen Reservoir projesiyle; özel, hibrit (karma) ve topluluk bulutlarını uygulayan ilk açık kaynak yazılım oldu (Rochwerger, 2009). Yine aynı yıl gerçek zamanlı bulut mimarileri ortaya çıkmaya başlamıştır.

2009 yılında ortaya çıkan Google Apps sayesinde kullanıcılar web ortamındaki uygulamalardan, kendi bilgisayarlarından bağımsız olarak sadece internet tarayıcısı aracılığıyla faydalanmaya başladılar. 2010 yılında Microsoft firmasının Azure isimli bulut bilişim hizmet platformu devreye alınmıştır.

2011 yılında açık ve özel bulutların birleşimi olan hibrit bulutlar ortaya çıkmış ve kullanılmaya başlanmıştır. Yine aynı yıl Apple firması kullanıcılarının, otomatik olarak ve kablosuz ortamda kişisel verilerini depolamalarına olanak tanıyan iCloud hizmetini kullanıma sunmuştur.

2012 yılında Google firması Google Drive'ı piyasaya sürerek, ücretsiz veri depolanmasına olanak sağlayan dosya depolama ve paylaşım platformlarına öncülük etmiştir.

2013 yılında IBM firmasının piyasaya sürdüğü Soft Layer Yazılımı ile kuruluşlara, özel bulut güvenilirliğinde, açık bulut mimarilerinin sağladığı işlem hızı ve maliyet tasarruflarını yakalama imkânı sağlanmıştır. Bu sayede kuruluşlar Servis olarak Altyapı (IaaS) satın almak suretiyle kendi bulutlarının performans ve ölçeklendirilebilirliğini esnek bir biçimde artırma imkânına kavuşmuştur.

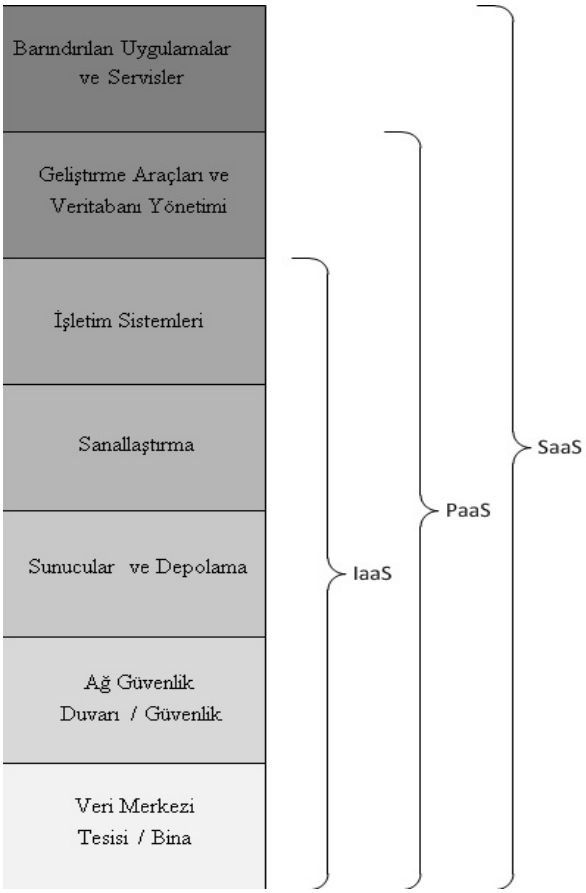
Günümüzde ise temel olarak eski internet mantığından çıkılarak, Web 2.0'ın sağladığı etkileşimli internetin benimsenmesi ve geleneksel mimariye uygun yazılan hizmet uygulamalarının bulut mimari altyapısına uygun hale dönüşmesi yönünde bir gelişim devam etmektedir.

1.4. Bulut Bilişim Servis Modelleri

Bulut bilişimin faydalandığı temel özelliklerden biri olan sanallaştırma vasıtasıyla, müşteriler ihtiyaçları doğrultusunda farklı bilişim kaynaklarını bulut sağlayıcılardan temin edebilirler. Bu kaynak bazen sadece depolama ünitesiyken, bazen de müşterinin faaliyeti ile ilgili geliştirmek istediği bir uygulama için bir geliştirme platformu olabilir. Bazı durumlarda ise bulut müşterisi bulut sağlayıcının servis ettiği uygulamayı kiralamak isteyebilir. Burada önemli olan müşterinin kaynak ihtiyacının çeşididir ve hizmet sağlayıcı bu ihtiyaca cevap vermek amacıyla ilgili kaynağı sanal olarak müşterisine sunar. Hizmet sağlayıcısının bilişim kaynağını müşteriye sunuş şekli veya seviyesine göre çeşitli servis modelleri ortaya çıkmıştır.

Bulut sağlayıcının sunum şekline göre çok sayıda servis modeli tanımlanabilse de, bulut bilişimde genel manada kabul görmüş ve diğer modelleri çatısı altında toplayan üç adet servis modeli bulunmaktadır. Bunlar sırasıyla Servis olarak Yazılım (SaaS), Servis olarak Yazılım Geliştirme Platformu (PaaS) ve Servis olarak Altyapı (IaaS)'dır. Bu bölümde bu üç temel bulut bilişim servis modeline ek olarak bazı kaynaklar tarafından bu hizmet modellerinden farklı özellikler gösterdikleri vurgulanan Servis olarak Haberleşme (CaaS) ve Servis olarak Ağ (NaaS) da incelenecektir.

Aşağıdaki şekilde temel bulut servis modellerinin kapsadığı hizmet başlıkları belirtilmiştir. Şekilden de anlaşılacağı üzere Servis olarak Altyapı (IaaS)'da müşteri veya kuruluş kendi kullanımı için gerekli bilişim altyapısını temin edebilirken, Servis olarak Yazılım (SaaS)'da sağlayıcının altyapısı üzerindeki bir uygulama veya yazılımı kullanmaktadır.



Şekil 1.2: Bulut Bilişim Servis Modelleri (Kaynak: Servicearchitecture.com)

1.4.1. Servis olarak Yazılım (SaaS)

Müşteriye, bulut altyapısı üzerinde çalışan sağlayıcının uygulamalarını kullanma yeteneği sağlar. Uygulamalara, çeşitli istemci cihazlar tarafından, web tarayıcı gibi ince istemci arayüzleri üzerinden erişilebilir. Müşteriler alt yapıda yer alan ağ, sunucular, işletim sistemleri, depolama ve hatta uygulamanın kendi yetenekleri de dâhil olmak üzere birçok kaynağı kontrol edemez ve yönetemez. Sınırlı kullanıcıya özgü uygulama yapılandırma ayarları bu durumun istisnası olabilir (Carstensen, 2012).

SaaS mimarisi erişim, kullanılabilirlik, performans ve güvenlik gibi hizmet özelliklerinin sorumluluğunun ve tüm kontrolün sağlayıcıda olduğu; müşterinin herhangi bir sorumluluğunun bulunmayıp sadece abonelik sistemiyle uygulamayla etkileşimde olduğu bir yapıdadır. Kullanıcılar ihtiyaçları doğrultusunda bir dizi uygulamayı internet erişimli cihazları üzerinden kullanabilirler. Muhasebe, faturalandırma, izleme, satış, planlama, performans izleme ve iletişim (webmail ve anlık mesajlaşma dâhil) gibi iş türleri ile ilgili uygulamaları bu mimari çerçevesinde kullanmak mümkündür.

SaaS servis modelinde yer alan uygulamalar genellikle tek bir kullanıcının işletmesi için değil de çoklu kullanıcıya tahsis edilirler. Tek bir uygulamanın birçok kullanıcı tarafından paylaşılması, uygulama güvenliğini ve farklı kullanıcıların birbirlerinin veri ve çıktılarını görüntüleyemediği uygulama kaynağı bölümlemesini kritik hale getirmektedir.

Güncel SaaS servis modellerine Google, Twitter, Facebook ve Flickr gibi sosyal paylaşım siteleri örnek olarak verilebilir ancak en çok kullanılan örnek internette Microsoft Live tarafından belli bir ücret karşılığında çoğaltılan Microsoft Office paketleridir.

SaaS mimarisinin sağladığı en önemli avantajları;

- Bütün altyapı bulut sağlayıcıda olduğundan ek bir donanım maliyeti gerektirmemesi,
- Uygulamalar tek bir abonelik sonrası kullanıma hazır olacağından ek bir ön kurulum maliyeti yaratmaması,

- Kullanıcıların, belirli bir süre için ihtiyaç duydukları bir yazılım için, kullandıkları süreye göre ücret ödeyebilmeleri ve ihtiyaçları bittiğinde aboneliklerini sonlandırabilmeleri,
- Kullanıcıların daha fazla bilişim kaynağı altyapısına ihtiyaç duymaları halinde bu kaynağı kendileri temin etmeden, sağlayıcıdan talep edip kısa sürede elde edebilmesi,
- Genellikle ücretsiz bir biçimde güncelleştirmelerin otomatik olarak yapılması,
- SaaS uygulamalarının web tarayıcısına sahip birçok farklı cihaz tarafından erişilebilmesi sayesinde platform bağımsız şekilde kullanılabilmesi,
- Uygulamaların belirli bir müşterinin ihtiyaçları doğrultusunda özelleştirilebilmesine olanak sağlaması,

olarak sıralanabilecektir.

1.4.2. Servis olarak Yazılım Geliştirme Platformu (PaaS)

Müşteriye, sağlayıcı tarafından desteklenen programlama dilleri ve araçlarını kullanarak oluşturduğu veya edindiği uygulamalarını, bulut altyapısı üzerinden sunma yeteneği sağlar. Müşteriler alt yapıda yer alan ağ, sunucular, işletim sistemleri veya depolamayı kontrol edemez veya yönetemez fakat yerleştirilen uygulamalar ve muhtemelen uygulama barındırma ortamı yapılandırmaları üzerinde kontrolleri vardır (Carstensen, 2012).

PaaS servisleri SaaS'te olduğu gibi, sağlayıcıya ait bulutlarda barındırılmakta ve müşterilerinin kendi web tarayıcıları üzerinden erişilebilmektedir. PaaS, IaaS ve SaaS servisleri ortasında tanımlanan bir servis türü olup, genellikle özellikli bir yazılım geliştirme amacı olmayan müşteriler SaaS servislerini kullanırlarken, yazılım geliştiriciler PaaS kullanmayı tercih etmektedirler. PaaS, uygulama programcılarına kod çalıştırma, veri depolama, kullanıcı kimlik yönetimi ve gerekli uygulama servislerini barındırmak için kullanabileceği yazılım araçları ve kütüphaneler sağlayarak, uygulama geliştirmesine olanak sağlar.

PaaS'ı, IaaS'tan ayıran en önemli özellik ise ölçeklendirmenin kullanıcı tarafından değil de sağlayıcı tarafından gerçekleştirilmesidir. Uygulamanın kullanım ihtiyacına bağlı olarak bilişim kaynağının içe ve dışa dönük ölçeklendirilmesi sorumluluğu sağlayıcıya ait olduğundan, yazılım geliştirici altyapı yapılandırma endişesi taşımadan geliştirdiği uygulamaya odaklanabilmektedir. Ayrıca, birçok uygulama geliştiricinin, geliştirdiği uygulamanın sisteme getirdiği yükün büyümesi sebebiyle kaynak ekleyip çıkarmaya veya ilgili uygulamayı bu işlemi otomatik olarak yapacak şekilde programlaya dönük bilgisi ve tecrübesi yoktur. Bu konuda tecrübeli yazılım geliştiricilerin birçoğu da bu iş için ayrıca vakit ayırmak istememektedirler.

PaaS servis sağlayıcıları kullanıcıların gelişen ihtiyaçları ve geri bildirimleri doğrultusunda platformları üzerinde periyodik olarak güncelleştirme yaparlar ve eski özelliklerin sürümlerini yükseltmek yanında yeni özellikler de eklerler. PaaS sağlayıcılar platformlarında uygulama geliştiren kullanıcılarına, yenilikçi fikirlerini geliştirme, uygulamalarını test etme ve yükleme gibi konularda yardımcı olabilirler. Yine web tasarımcıları PaaS servislerini tasarım sürecini geliştirme, test ve işin sonunda web sitelerini barındırmak amaçlarıyla kullanabilirler.

PaaS mimarisinin sağladığı en önemli avantajları;

- Yazılım geliştirme alanında uzman olmasa dahi kullanıcıların belli ölçekte uygulamalar geliştirmesine imkân sağlayan araçlar ve kütüphaneler sunması,
- Kuruluşların ve diğer müşterilerin herhangi bir fiziksel altyapı harcaması yapmadan ve fiziksel altyapıyı yönetecek uzman personele ihtiyaç duymadan; kendi ihtiyaçları kadar bilişim kaynağını kiralayarak yazılım geliştirmelerine olanak tanıması,
- Müşterilerine, uygulama geliştirdikleri araçların kontrolüne sahip bir şekilde, platformun sağladığı özelliklerden istediklerini serbestçe seçerek kendi gereksinimlerine uygun yazılım geliştirme imkânı tanıması,
- Kullanıcıların gereksinimleri paralelinde platform özelliklerinin değiştirilebilmesi,

- Platform bağımsız çalışılabilmesi sayesinde farklı lokasyonlardaki birçok yazılım geliştiricinin aynı uygulama üzerinde takım halinde çalışabilmesine olanak sağlaması,
- Veri güvenliği, yedekleme ve kurtarmanın sağlayıcı tarafından gerçekleştirilmesi,

olarak sıralanabilecektir.

1.4.3. Servis olarak Altyapı (IaaS)

Müşteriye, isteği doğrultusunda işletim sistemleri ve diğer uygulamalar gibi yazılımlar yüklemesinin ve çalıştırmasının mümkün olduğu işlemci, depolama, ağ ve diğer bilişim kaynaklarını tedarik etme yeteneği sağlar. Tüketici bulut altyapısını kontrol edemez ve yönetemez fakat işletim sistemleri, depolama üniteleri ve uygulamalar üzerinde kontrole ve muhtemelen seçilen ağ bileşenleri (örneğin sağlayıcı güvenlik duvarı) üzerinde sınırlı denetime sahiptir (Carstensen, 2012).

IaaS mimarisi müşterilerine, ihtiyaç duydukları ölçekte sanal sunucu alanı, ağ bağlantıları, bant genişliği, IP adresleri ve yük dengeleyici gibi bilişim kaynaklarını bulut sağlayıcıların altyapıları üzerinden kullanma imkânı sunar. Fiziksel olarak bu kaynaklar, bulut sağlayıcısının sahip olduğu çok sayıda veri merkezine dağıtılmış vaziyetteki çok sayıda sunucu ve ağdan oluşan donanım kaynak havuzundan çekilir ve bütün altyapının işletilmesi ve devamlılığını sürdürmesi tamamen bulut sağlayıcısının sorumluluğundadır. Müşteri yanlızca kendisine tahsis edilen sanal kaynaklara erişir ve bu kaynaklar üzerindeki işlem kapasitesini kullanır. Kullanılan kaynaklar için en yaygın kullanılan ödeme çeşidi kullandığın kadar öde modelidir. Genel olarak sanal makine kapasitesine bağlı olarak saatlik ücret politikası uygulanır.

IaaS mimarisinin sağladığı en önemli avantajları;

- Ölçeklenebilir yapısı sayesinde, bilişim kaynağı ihtiyacının arttığı durumlarda temin süresi beklemesine meydan vermeden hızlıca kaynağın artırılabilmesi ve

kullanılmayan kaynağın salıverilebilmesi yoluyla kapasite israfının önüne geçilmesi,

- Donanım yatırımına ihtiyaç duyulmaması ve böylece müşterinin yatırım süresi ve maliyetinden tasarruf sağlaması,
- Kullandığın kadar öde prensibiyle müşterinin sadece gerçekten kullandığı kaynağın ücretini ödemesine olanak tanıması,
- Altyapının çok fazla sayıda müşteriye hizmet veren veri merkezilerinde barındırılması sayesinde, ilgili veri merkezlerinin hem siber ve hem de fiziksel güvenlik açılarından müşterilerin kendi kuracakları göreceli olarak küçük veri merkezlerine göre çok daha iyi korunabilmesi,
- Bulut sağlayıcının sahipliğindeki bir sunucu hatta veri merkezlerinden birinin arıza vermesi durumunda bile, donanım kaynakları fazlalığı ve konfigürasyonların yedekliliği sayesinde servisin etkilenmemesi ve çalışmayı sürdürebilmesi,
- Müşterilerin kullandıkları bilişim kaynaklarının tedariği, işletilmesi ve bakımı gibi sorumluluklarını tamamen bulut sağlayıcısına aktarmaları sayesinde, bu iş ve işlemler ile ile ilgili uzman çalışan bulundurma ihtiyaçlarını ortadan kaldırması,

olarak sıralanabilecektir.

IaaS mimarisi kuruluşlar tarafından kendi iç bilişim hizmetleri için altyapı olarak, dış kullanıcılara servis edecekleri bulut uygulamalarını veya web sitelerini barındırmak veya yine kendi daha küçük ölçekli müşterilerine altyapı sağlamak amaçlarıyla kullanılabilir. Halen genel olarak kabul görmüş olmasa da, kuruluşların kendi varlık kaynaklarını kullanmak yerine harici kaynakları kullanmasının, fiziksel donanım temin ve işletme maliyetleri dikkate alındığında daha ucuz olacağı yönünde kanıtlar vardır. Bu sebeple de günümüzde birçok kuruluşta bilişim altyapılarını harici sağlayıcılardan temin etme eğilimi görülmektedir.

1.4.4. Diğer Bulut Bilişim Servis Modelleri

Genel olarak kabul görmüş servis modelerine ek olarak bazı kaynaklar Servis olarak İletişim ve Servis olarak Ağ hizmet modellerini ayrıca ele alır. Bu servislere burada kısaca değinilecektir.

Servis olarak İletişim (CaaS): CaaS, sabit ve mobil cihazlar kullanılarak, IP üzerinden ses (VoIP ve internet telefonu), anlık mesajlaşma (IM), tümleşik iletişim, yayıncılık ve video konferans uygulamaları gibi hizmetleri içeren dış kaynaklı kurumsal bir iletişim çözümüdür. Bu hizmet modelinde SaaS hizmet modelinde olduğu üzere sağlayıcı tüm donanım ve yazılım çözümlerini sağlamakla yükümlüdür. Müşteriler yine kullandığın kadar öde modeliyle iletişim aygıtları ve çözümlerine erişebilirler. Böylece örneğin bir kuruluş kendi video konferans altyapısını kurma maliyetinden kurtularak bu hizmeti sağlayan firmadan kiralayabilir. Sistem talep üzerine genişleyebilecek esneklikte olup, yeni cihazlar kolayca eklenebilir. Eklenen yeni cihazlara göre ağ kapasitesi ve özellik kümeleri otomatik olarak değiştirilebilir ve böylece kaynak israfı engellenebilir.

Servis olarak Ağ (NaaS): NaaS ağ bağlantısı taşıma hizmetleri içeren bir servis modelidir. NaaS ağ ve bilgisayar kaynaklarının bir bütün olduğunu göz önünde bulundurarak, kaynak paylaştırmaya yönelik optimizasyonlar içerir (Gabrielsson, 2010). NaaS özetle müşterilere, ağ altyapısının sahipleri tarafından, sanal ağ hizmeti sağlanması demektir. Bunun için genellikle OpenFlow ağ sanallaştırma protokolleri kullanılır.

NAAS servis modelleri esnek ve uzatılmış sanal özel ağlar (VPN), bant genişliği, özel yönlendirme, çoklu yayın protokolleri, güvenlik duvarı, saldırı tespit ve önleme yazılımları, geniş alan ağı (WAN), içerik izleme, filtreleme ve antivirüs hizmetleri verebilirler. Bazı kaynaklarda IaaS servis modeli içinde yer alan bu servis modelinin içeriğine ait standartlar henüz belirlenmemiştir.

1.5. Bulut Bilişim Mimari Çeşitleri

Bulut mimari çeşitleri bulut ortamının ne şekilde düzenleneceği ve servis edileceği ile ilgili farklı yaklaşımlardır. NIST'e göre (Mell ve Grance, 2009) dört genel

yaklaşım vardır ve bunlar Açık (Public), Özel (Private), Hybrid (Hibrit) ve Topluluk (Community) bulutları olarak adlandırılmaktadır.

1.5.1. Açık (Public) Bulut

Açık bulut mimarisi, bulut bilişim en çok tanınan modeli olup; bünyesinde bulunan bulut hizmetleri, sanallaştırılmış bir ortamda toplanmış ve paylaşılan fiziki kaynaklar kullanılarak inşa edilirler ve internet gibi ortak bir ağ üzerinden erişilebilirler. Bu mimari çeşidi bulut bilişimin getirdiği yenilikçi özelliklerin hemen hemen tamamına sahiptir.

Açık bulut servislerine, bulut depolama ve çevrimiçi ofis uygulamaları gibi Servis olarak Yazılım (SaaS) servisleri başta olmak üzere, yaygın olarak kullanılan bulut tabanlı web barındırma (IaaS) ve yazılım geliştirme ortamları (PaaS) örnek olarak gösterilebilir.

Bir açık bulutta bulunan hizmetler, servis sağlayıcılar tarafından barındırılır ve yönetilir. Bu durumda kurulum, yönetim, tedarik ve bulutun bakımı ve orada ikamet eden hizmetler için sorumluluk bulut sağlayıcısınındır. Bu bulut mimarisi her türlü kamu ve özel sektör kuruluşları tarafından kullanılmak üzere tasarlanmıştır. Çok kiracılı ortamları destekleyen kapsamlı bulutlar olup; son derece verimli, otomatik ve sanallaştırılmış altyapılar üzerine inşa edilirler. Tüketiciler, kullandığın kadar öde prensibiyle sadece kullandıkları kaynaklar ve hizmetler için ücretlendirilirler. Bulut sağlayıcılarının durumun bilincinde olmasına ve sistemlerini korumak için yeni teknoloji ve araçları edinmesine rağmen, yeterli güvenlik ve yasal uyumluluk eksikliği genellikle bu mimarinin önemli bir konusudur (Mahmood, 2015).

Açık bulutta sağlayıcı ticari bir kazanç beklentisi içinde olduğundan, belli bir zamanda kullandırabileceği bilişim kaynağı miktarının fiziksel bir limiti olacak olup; eğer müşterisi ile arasında kullanım miktarını belirleyen bir hizmet seviye anlaşması mevcut değilse ve alınan hizmet için bu yönde ekstra bir ücret ödenmiyorsa, hizmeti minimum seviyede kullandırmayı tercih edecektir.

Hizmet seviye anlaşmaları genelde kullanıcıya bilişim kaynaklarının fiziksel olarak ne şekilde sağlanacağını dair bir kontrol veya söz hakkı tanımaz. Kullanıcı sadece paylaştırılmış kaynaklar üzerinde sanal olarak kendisi için ayrılmış kaynağı kullanır. Burada bulut sağlayıcısının fiziksel olarak birçok farklı lokasyondaki veri merkezinde tuttuğu kaynaklarının sanallaştırılmış havuzundan belli oranda kaynağı kullanıcıya sunduğu düşünüldüğünde, kullanıcının verisinin fiziksel olarak nerede tutulduğunu bilme ve kontrol etme şansı ortadan kalkmaktadır. Ayrıca bu kontrol eksikliği, servis sağlayıcı personelinden bir kişinin uygunsuz şekilde kullanıcının verilerine erişmesini mümkün kılar. Bu durum güvenlik kaygısı taşıyan birçok kuruluşu kendi özel bulutlarına (private cloud) sahip olmaya sevk etmektedir.

1.5.2. Özel (Private) Bulut

Özel bulut genellikle, belirli bir kuruluş için tasarlanmış özel bir ağ ve veri merkezinden ibarettir. Bu mimari kuruluşun veya belli bir kullanıcı grubunun özel kullanımı içindir. Özel bulutlar da, açık bulutlar gibi yüksek verimli, otomatik ve sanallaştırılmış altyapılar üzerine inşa edilmiş, çoklu-kiracılı ortamlardır. Yalnız bu mimaride, bulutun kurulması ve idame ettirilmesinin kontrolü tamamen kullanıcı kuruluşa aittir. Bu nedenle güvenlik denetimi, yasal uyumluluk ve hizmet kalitesi kuruluşun kendi ihtiyaçlarına göre belirlenebilmekte ve açık bulutlara oranla çok daha iyi bir şekilde sağlanabilmektedir. Bir servis sağlayıcı özel bir bulut oluşturmak için açık bulut kaynaklarını kullanırsa elde edilen ortam, sanal özel bulut olarak adlandırılmaktadır (Mahmood, 2015).

Özel bulut mimarisinde altyapı kuruluşun yerel veri merkezinde tutulabileceği gibi, bu kuruluş adına üçüncü bir tarafça da barındırılabilir. Bu altyapıya, özel kiralık hatlar veya güvenli şifre bağlantılı açık ağlar üzerinden erişilebilir. Örneğin Google şirketinin Amerika Birleşik Devletleri'ne sunduğu hizmette, kamu kuruluşlarının verilerinin Amerika Birleşik Devletleri sınırlarındaki belli veri merkezlerinde tutulacağı ve ilgili veri merkezlerinde görev alacak personelin ekstra özgeçmiş kontrolünden ve güvenlik taramalarından geçirileceğini taahhüt edilmektedir.

Varlık merkezinin tüm kontrolü, mülkiyet veya sözleşme yoluyla varlık sahibi kullanıcı kuruluşun elinde olduğundan, gizlilik ve güvenlik gibi riskler sebebiyle açık bulut mimarisi kullanmaktan kaçınan finansal hizmet kuruluşları veya devlet kurumlarının kullanımı için daha uygun mimarilerdir. Kuruluşlar özel bulutları kendi iç iş akışları için kullanabilecekleri gibi, kendi müşterilerine hizmet sunmak amacıyla da kullanabilirler.

Günümüzde birçok kuruluş hem açık hem de özel bulutları kullanmaktadır. Gizlilik seviyesi yüksek veya yasal olarak paylaşılması hukuki olmayan verilerin barındırılması veya ilgili işlemlerin gerçekleştirilmesi için özel bulutlar kullanan kuruluşlar, bu şekilde kısıtları olmayan halka açık işlemleri için açık bulut altyapılarından faydalanabilmektedir. Depolanan ve işlenen verilerin hassasiyetinin yüksek olduğu durumlarda sadece bu özel durumlar için tahsis edilmiş fiziksel sunucular veya ayrılmış ağ bağlantıları kullanılabileceği gibi; gizliliğin seviyesine göre, açık bulut altyapısının geri kalan kısmından soyutlanarak tamamen ayrı bir altyapının oluşturulduğu sanal özel bulutlar da kullanılabilir. Sanal özel bulutlar maliyet olarak açık bulutlara kıyasla daha pahalı olsalar da, kuruluşların kaynaklarını kendi veri merkezlerinde barındırdıkları özel bulut uygulamalarına göre önemli oranda maliyet avantajı sağlarlar.

Özel bulutların, açık bulutlara göre daha lokal ve dolayısıyla kaynaklar bakımından daha mütevazi olması ve bu kaynakların da sadece belli ve sınırlı amaçlara hizmet eden bir havuzda toplanması; bu mimaride kaynakların ölçeklendirilebilirlik düzeyini ve sonuç olarak verimliliğini azaltmaktadır.

1.5.3. Hibrit (Hybrid) Bulut

Hibrit bulutlar, iki ya da daha çok farklı bulut mimari çeşidinin kombinasyonudur. Genellikle özel ve açık bulut mimarileri bir arada kullanılır. Bu durumda hibrit bulut, kendi içindeki özel bulut ile uyumlu bir şekilde talep edilen dış kapasiteyi açık buluttan sağlar. Yönetim sorumlulukları kendi özel bulutuna sahip kuruluş ve açık bulut sağlayıcısı arasında bölünür. Bu sorumlulukların sık sık çakışması

ve karşılıklı güven sınırlarının belirsizliği endişe verici bir sorunlar haline gelebilmektedir. Kuruluşun kendisi tarafından geliştirilen kontrol ve yönetim mekanizmaları sayesinde, kritik iş süreçleri için bu mimari çok daha etkilidir ancak göreceli olarak açık buluta göre daha pahalıdır. Hibrit bulut kullanmanın temel avantajı, kritik ve özel uygulamalar ve veriler özel bulutta tutulabilirken aynı anda daha az kritik genel hizmetler ve uygulamaların açık bulutta bulunabilmesidir (Mahmood, 2015).

Hibrit bulut mimarisinde tek bir bulut mimarisi gibi çalışan iki farklı bulutun senkronizasyonu önem arz etmektedir. Özel bulutta gerçekleştirilen işlemlerin sonucu olarak üretilen verilerin belirli bir kısmı açık bulutta tutulan uygulamaların girdileri olabileceği gibi, tam tersi bir durum da söz konusu olabilir. Hibrit bulut mimarisinin, iki farklı lokasyonda gerçekleştirilen işlemler arasındaki işbirliği ve senkronizasyonu otomatik olarak sağlayacak şekilde tasarlanması gerekmektedir. Bu mimaride genelde hibrit bulutun özel bulut katmanında çalışan uygulama ve servisler, açık bulutta bulunan altyapıyı veya uygulamaları yönetmekte ve kuruluşun kendi altyapısının yetersiz kaldığı durumlar için gerekli kaynağı açık bulut sağlayıcısından temin etmektedirler.

Hibrit bulut modelleri, bireysel bulut sağlayıcıları tarafından bir hibrit paket halinde sunulabileceği gibi, farklı bulut sağlayıcıların bir ekip halinde özel ve açık servisleri tek bir entegre servis şeklinde sağlamaları veya kendi özel bulutlatını yöneten kuruluşların kendi altyapılarına entegre edecekleri bir açık bulut hizmetini temin etmeleri şekillerinde de sunulabilir.

Hibrit bulut mimarileri genellikle benzer hizmet için, güvenlik ve gizlilik gereksinimleri dikkate alınarak iki farklı bulutun birlikte çalıştırıldığı mimarilerdir. Örnek vermek gerekirse, bir e-ticaret sitesi güvenli bir altyapı sunması sebebiyle özel bulutta, bu siteye ait tanıtım sitesi ise uygun maliyetli olması sebebiyle açık bulutta barındırılabilir. Servis olarak Altyapı (IaaS) sunan bir sağlayıcı, müşteri verilerini özel bir bulutta tutmaya yönelik bir hizmet sağlayabilir ancak aynı anda açık bulutta herhangi bir lokasyondan birden fazla kullanıcı tarafından erişilebilecek şekilde, proje planlama dokümanlarının kullanımına izin verebilir.

1.5.4. Topluluk (Community) Bulutu

Bu mimari bir açık/özel bulutların özel bir halidir. Her ne kadar, özel olarak belirli bir kuruluş için kullanılmasalar da, aynı düşüncedeki insanların/topluluklar için örneğin bilim adamları için, tıp mesleğini icra edenler için, bilimsel araştırma amaçlı ya da bir kamu bulutu olabilecek şekilde tasarlanırlar. Bu bulut ortamı oldukça geneldir fakat açık bulutlar gibi herkese açık değillerdir. Güvenlik derecesi bakımından özel bulutlar kadar titiz değillerdir fakat bir topluluk bulutunun tüketicilerinin aynı ya da benzer gereksinimleri olduğu düşünüldüğünde açık bulutlardan daha iyidirler.'Topluluk' bulutun sahibi olup ve bulutu yönetir, ancak bir üçüncü taraf da 'topluluk' adına bulut oluşturmak ve yönetmek için kullanılabilir (Mahmood, 2015).

Topluluk bulutları ortak amaçları olan kullanıcılardan oluştuğu için, kullanıcıların güvenlik ve uyumluluk politika ve gereksinimleri benzerlik göstermektedir. Ayrıca genelde kullanıcılar benzer sektörlerde veya çalışma gruplarında olduklarından, bu kişilerin kullanımına yönelik uygulamalar, yazılım platformları ve diğer altyapılar topluluk bulutlarında daha özelleşmiş ve gelişmiştir.

Açık bulut mimarisinden faydalanılarak oluşturulan topluluk bulutları, açık bulut sağlayıcısından kiralanan bilişim kaynaklarının, topluluğun faaliyet alanı çerçevesinde düzenlenip, topluluğun kullanıcılarına sunulması şeklinde faaliyet gösterirler. Özel bulut mimarisinden faydalananlarda ise, genellikle benzer sektörlerdeki kuruluşlar, kendilerine ait bilişim kaynaklarını tek bir havuzda toplayarak, sektörel bir hizmetin sunulmasına yönelik bir topluluk bulutu oluştururlar.

1.6. Bulut Bilişim Donanım ve Yazılım Katmanları

Bulut bilişim mimarilerinin donanım ve yazılım bileşenleri, çoğunlukla geleneksel veri merkezi mimarilerine benzemekle birlikte; uygulamada güvenlik, erişilebilirlik ve kullanılabilirlik vb. birçok açıdan önemli farklılıklar göstermektedir. Ortaya çıkan farkların önemli bir bölümü, bulut bilişim ortamının işletilebilmesine yönelik geliştirilen yazılım teknolojilerinden kaynaklanmaktadır. Sanallaştırmanın

uygulama ortamını uzaktaki fiziksel sunuculardan soyutlaması, statik bilişim ortamları için geliştirilmiş yazılımların işlevlerini yitirmesine neden olur. Ayrıca bulut mimarilerinde öne çıkan otomatik yönetim özelliği; manuel yönetim uygulamaları olan geleneksel tarzdaki yazılım ürün, bileşen ve bunların yapılandırmalarını bulutun dinamik yapısına uyumsuz hale getirir. Bulut ortamındaki fiziksel bilişim kaynakları, geleneksel mimarideki gibi belli işlemler için tahsis edilmek yerine, birçok değişken işlem için dinamik bir şekilde ayrılabilecek kaynak havuzlarına dönüşmektedir. Diğer bir fark ise bulut ortamlarında özellikle veri güvenliğine ilişkin sorumluluğun paydaşlar (sağlayıcı, müşteri) arasında paylaşılmasıdır. Bu sebeple bulut bilişim mimarisini meydana getiren bileşenleri, bu mimarinin kural ve gereksinimlerini göz önüne alarak incelemek faydalı olacaktır.

1.6.1. Bulut Bilişim Donanım Katmanı

Bulut bilişimin altyapısını oluşturan donanımlar, geleneksel mimarilerdeki benzerlerinden belli başlı farklılıklar taşımaktadır. En önemli farklardan biri, geleneksel mimarilerde donanımların belli bir fiziksel veri merkezinde toplanarak sınırlı sayıda kullanıcıya hizmet vermesiyken, bulut bilişimde farklı lokasyonlardaki veri merkezlerindeki bilişim kaynaklarının tek bir havuzda toplanarak çoz fazla sayıda kullanıcıya daha verimli hizmet sağlamasıdır.

Bulut bilişim donanım katmanı bileşenlerini kısaca aşağıdaki şekilde açıklayabiliriz:

Dış ağ ve internet bağlantısı: Bulut bilişimin önemli bir özelliği olan yüksek kullanılabilirlik için, bulut altyapısının normalde her biri farklı bir sağlayıcıdan olmak üzere iki internet bağlantısı olması gerekmektedir. Buna ek olarak, olası hizmet kesintilerini engellemek amacıyla veri merkezi tasarımında her iki bağlantının farklı bir taraftan veri merkezi binasına gelmesi, her iki bağlantının aynı anda kesilmesini engelleme açısından önemlidir. Internet bağlantısı yanı sıra, veri merkezinin belirli kullanıcıları arasında doğrudan, özel bağlantı sağlamak için ilave ağ bağlantıları

kullanılabilmektedir. Kullanılan ağların çeşitlendirilmesi herhangi bir arıza nedeniyle hizmetin aksamasının engellenmesi açısından önem taşımaktadır.

Dâhili ağ altyapısı: Bireysel bilişim cihazlarının yarattığı ağ trafiği, paylaşılan bir ağ altyapısı üzerinde çalışmaktadır. Bu altyapı tamamen veri merkezinin iç işleyişi ve bilişim kaynaklarının tek hazvuzda toplanmasına yönelik olup, güvenliği ve performansı sağlayıcının sorumluluğundadır.

Sunucular: Sunucular, bütün işlemleri gerçekleştiren cihazlardır. Bulut bilişim ortamında bir sunucu, dağınık farklı kullanıcılar tarafından kullanılan bir dizi sanal makineyi destekler. Başka bir deyişle sunucular, bulut yönetim yazılımı tarafından kendilerine tahsis edilen sanal makineler tarafından kullanılan ve paylaşılan kaynaklardır. Bulut bilişim veri merkezleri, çok sayıda sunucunun birleşimi ile oluşmuş çok büyük sunucu kümeleridir.

Depolama Aygıtları: Her sanal makine, üzerine verilerini yerleştirdiği depolama aygıtı kullanır. Burada veriler kullanıcının sorumluluğundayken, depolama aygıtının işlevselliği sağlayıcı sorumluluğundadır. Bazı bulut sağlayıcıları kullanıcı verilerini depolamak için yerel olarak bağlı disk sürücüleri kullanabilmekteyse de, depolama genellikle veri merkezlerinin depolama altyapısına bulunur.

Ağ bağlantısı: Her bir sunucunun veri iletmek ve ağ altyapısından veri almak için bir veya daha fazla ağ arayüz kartı vardır. Bir ağ arayüz kartı, sunucuların ağa özel ve tam zamanlı bağlantı kurmasını sağlar.

1.6.2. Bulut Bilişim Yazılım Katmanı

Yazılım altyapısı bulut bilişime işlevsellik sağlamak için kullanılan ve altyapıya yerleştirilen uygulamaları destekleyen yazılımlardan oluşur. Bulut bilişimi mimarilerini geleneksel mimarilerden ayıran temel farklar, yazılım katmanı bileşenlerinde ortaya çıkmaktadır. Bulut bilişim yazılım katmanının bileşenlerini kısaca aşağıdaki şekilde açıklayabiliriz:

Hipervizörler: Fiziksel sunucular ile bu sunucular üzerinde çalışan sanal makineler arasında bulunan bir yazılım katmanıdır. Hipervizörler sanallaştırmanın temelini oluştururlar ve fiziksel donanımdan istenen özelliklere sahip mantıksal donanımlar oluştururlar. Bu yazılımların yüklenmesi, konfigürasyonu, sonraki yükseltme ve güncellemeleri, yama yüklenmesi ve kodların özelleştirilmesi gibi işlemlerin sorumluluğu sağlayıcıya aittir.

Hipervizörler iki çeşide ayrılırlar. Birinci çeşit hipervizör, gerçek donanımlar üstüne kurulan işletim sisteminden oluşur. İkincisi çeşit ise sadece hipervizör yazılımından oluşur. Birinci çeşit sanallaştırma yazılımı kendi içerisinde bir işletim sistemi barındırdığından dolayı kullanımı kolaydır fakat güvenliğini sağlamak için fazladan önlemler alınması gerekir. İkinci çeşit hipervizörde ise bir işletim sistemi bulunmadığından fiziksel donanıma erişim ve işletim birincisi kadar kolay değildir, fakat bir işletim sistemi barındırmadığından alınması gereken güvenlik önlemleri ilki kadar fazla değildir (CISN, 2015).

Bulut yönetim yazılımı: Bir bulut yönetim yazılımı, bulut tabanlı ve dâhili iş birimleri arasındaki bağlantıları ve etkileşimleri yöneten programdır. BT bağlamında bu yazılımlar, yapılacak görevleri iş akışları şeklinde birleştirerek, çeşitli BT bileşenleri ve bunlarla ilişkili kaynakların yapılandırılmasını ve yönetimini otomatik hale getirilebilirler. Bulut bilişim, birden çok farklı lokasyondaki heterojen sistemler üzerinde çalışan birbirine bağlı süreçler içerdiğinden, bu durum (otomatik yönetim) bulut ortamında daha karmaşıktır. Bulut yönetim yazılımı ürünleri, diğer kullanıcılar ve uygulamalar arasındaki bileşenlerin iletişim ve bağlantılarını basitleştirirler ve bu bağlantıların doğru yapılandırıldığından ve korunduğundan emin olunmasını sağlarlar.

Bulut yönetim yazılım ürünlerini değerlendirirken, ilk olarak mevcut ve katılan uygulamaların iş akışlarının haritalanması tavsiye edilir. Bu şekilde bir uygulama için dâhili iş akışının ne kadar karmaşık olduğu ve bilgilerin ne sıklıkla uygulama bileşenleri kümesinin dışında aktığını görselleştirilebilecektir (Service Architecture, 2015).

API yazılımı: Bulut servis sağlayıcıları arayüzler aracılığıyla hizmetlerine erişim sunarlar. Bu arayüzler genellikle API (uygulama programlama arayüzü) olarak adlandırılmakla beraber, bir programlama arayüzünden daha ziyade HTTP gibi ortak bir protokol kullanılarak internet üzerinden erişilebilen bir online hizmet de olabilir. Çoğu bulut sağlayıcısı için, bu online arabirimler hizmetleri ile etkileşimin temelidir ve bu API'lerin kullanılabilirliği ve güvenilirliği, hizmeti ayakta tutmak ve çalışmasını idame ettirmek açısından önemlidir.

Portal yazılımı: Bulut sağlayıcıların birçoğu, kullanıcıların altyapıyı etkin şekilde kullanmalarına imkân veren çevrimiçi tarayıcı arayüzleri sunarlar. Bu arayüzler, sanal makineleri başlatma, durdurma veya askıya alma, belirli sanal makinelere IP adresi atama, yük dengeleyici atama ve benzeri görevlere sahiptir. Bulut sağlayıcıları, sağladıkları hizmetin API'sini kullanması ve sundukları hizmete tüm diğer programlar gibi erişebilmesi sebebiyle, kendi portal yazılımlarının kullanıcılar tarafından kullanılmasını tercih ederler. Ancak birçok kullanıcı kendi bulut kaynaklarını yönetmek için harici bir araç kullanmayı tercih etmekte veya başka bir deyişle, kaynakları elde etmek ve serbest bırakmak için direkt sağlayıcı ortamı ile etkileşimde olan kendi uygulamalarını temin etmektedirler (Carstensen, 2012).

Sistem servisleri: Bulut sağlayıcıları bulut ortamının bir parçası olarak, daha etkin kullanımı sağlamak amacıyla, yazılım bileşenleri veya hizmetleri sunar. Örnek olarak, Amazon firmasının Web Servis uygulamalarını kullanmak için sunduğu mesaj kuyruğu hizmeti verilebilir. Bu hizmetler ile ilgili olarak uygulama geliştiricinin herhangi bir sorumluluğunun olmaması ve bu servisleri geliştirme işleminde etkin bir şekilde kullanması, geliştirme işlemini basitleştirir ve dolayısıyla zaman ve maliyet tasarrufu sağlar (Carstensen, 2012). Bu hizmetlerin kullanıcılara aktarılması, uygulama geliştiricilere yalnızca kendi uygulamanın tasarımına odaklanma ve tasarım için gerekli altyapıyı kurma çabasından kaçınma imkânı tanır.

Sistem izleme yazılımı: Bir bulut ortamı, işlem kaynaklarının (sunucular, depolama aygıtları, ağ cihazları, yazılım bileşenleri, vb.) büyük ve karmaşık bir havuzudur. Bu

kaynakların optimal çalışma sürelerini belirlemeye ve performanslarını arttırmaya yönelik olarak sürekli izlenmesi gerekir. Bu amaçla geliştirilen izleme platformları; son kullanıcı, uygulama, veritabanı ve altyapı arasındaki spesifik işlem ilişkilerinin, gerçek zamanlı olarak uçtan uca görüntülenmesini sağlar. Bu sayede sağlayıcıların sistemin eksik ve geliştirilmesi gereken yönleri hakkında bilgi edinmesi sağlanır.

Denetim ve personel izleme yazılımı: Bu tip yazılımlar bulut bilişimin işlevselliğine katkı sunmaz ve sistemin başarısını etkilemezler. Burada amaç sadece sağlayıcı için çalışan ve bulut ortamı ile bir şekilde etkileşim içinde olan kişileri izlemektir. Son kullanıcılar; diğer kuruluşlar ve özellikle de aynı sektördeki rakip kuruluşlar tarafından verilerine erişim sağlanması, bulut ortamında barındırdıkları kişiye özel bilgilerin üçüncü kişiler tarafından elde edilmesi vb. birçok risk sebebiyle uygulamalarını korumak için bulut sağlayıcıya bağlıdırlar. Ancak bu noktada son kullanıcıların, bulut servis sağlayıcısı çalışanlarının verilerine uygunsuz erişim sağlayabileceğine yönelik tereddütleri vardır. Bu sebeple birçok bulut sağlayıcısı, çalışanlarının anahtar sistem bileşenleri ile etkileşimini izlemek ve sadece yetkili personelin bu bileşenlere erişim sağlayabildiğinden emin olmak için izleme yazılımları kullanmaktadır. Bu izleme yazılımı kayıtları incelenerek, bulut ortamında herhangi bir yetkisiz aktivitenin gerçekleşip gerçekleşmediği kolayca anlaşılabilir (Carstensen, 2012).

İşletim sistemi: İşletim sistemleri, kullanıcının uygulamasının üzerinde çalıştığı paket yazılımlardır. Bu yazılımlar kullanıcının kendi veri merkezindeki bir fiziksel sunucu üzerinde çalışabileceği gibi, bulut mimarisinin çeşidine göre, bulut servis sağlayıcısının ortamında da bulunabilirler. İşletim sistemleri uygulama kodunu etkinleştirerek, uygulamayı çalıştırmak için yüklenen yazılım servisleridir. Uygulamanın başlatılması ve uygulama kodunun çalıştırılması ile birlikte süreç planlaması ve dosya sistemlerinin depolanması görevlerini de yerine getirirler.

Bulut bilişim ortamında ve özellikle de IaaS mimarilerinde, işletim sisteminin güvenliği ve kullanılabilirliği kullanıcının sorumluluğundadır. Bu yazılımla ilgili,

uygulamanın daha verimli çalışmasına yönelik olarak gerekli yükseltmeler, yamalar, yapılandırma ve diğer işlemler kullanıcı tarafından yerine getiririlir.

Ara katman yazılımı: Ara katman yazılımları iki farklı uygulama veya cihaz arasında bulunan yazılım platformlarıdır. Farklı iki kullanıcı, sunucular, veritabanları ve uygulamalar arasındaki bağlantıyı sağlar fakat son kullanıcılar tarafından doğrudan kullanılmaz. Bu yazılımlara örnek olarak veritabanı yazılımları, mesaj kuyrukları, uygulama sunucuları ve uygulama geliştirme çerçeveleri verilebilir.

Bulut ara katmanları genellikle işletim sistemi ve bir uygulama arasında yer alarak kullanıcıya bir dizi faydalar sağlarlar. Bir iş uygulaması geliştirilmesine yönelik olarak eş zamanlılığı, işlemleri, mesajlaşmayı kolaylaştırır ve servis odaklı mimari (SOA) uygulamaları oluşturmak için gerekli olan servis bileşeni mimari çerçevesini sağlarlar. Bu yazılımlar genellikle haberleşme hizmetleri sunarlar ve farklı uygulamalar arasında iletileri göndermek ve almak adına bir haberci gibi hizmet verirler. Fiziksel olarak farklı mekânlarda yer alan farklı uygulamalar, bulut ara katmanı sayesinde birlikte bir görevi gerçekleştirmek için entegre edilebilirler (Technopedia, 2016).

Uygulama kodu: Uygulama kodu, uygulamanın gerçek işlevselliğini sağlayan yazılım bileşenlerinden oluşur. Bu kod java bileşenleri veya web sayfaları şeklinde olabilir. Uygulama kodunun tamamen kullanıcının geliştirdiği bir bileşen olması sebebiyle güvenliğine ve çalışmasına yönelik sorumluluk tamamen kullanıcınındır.

Diğer uygulama bileşenleri: Karmaşık uygulama topolojilerinde, uygulama bileşenleri diğer sanal makinelerde bulunabilirler. Bu bileşenlere örnek olarak önbelleğe yazılım alma, yük dengeleyici bileşenleri ve son kullanıcıları ücretlendirmek için geliştirilen fatura yazılımları verilebilir. Bu bileşenler işletim sistemi düzeyinde değil de, uygulama düzeyinde işlevsellik sağlarlar. Bulut kullanıcısı tarafından yazılım paketleri olarak yüklenmiş olabilecekleri gibi, önceden yapılandırılmış bir sanal makine şablonu şeklinde bileşen yaratıcısı tarafından sağlanabilirler.

Bu bileşenler ister kullanıcı tarafından yüklenmiş, isterse de bir uygulama yaratıcısı tarafından oluşturulmuş bir şablondan kullanıcı tarafından başlatılmış olsunlar; bulut sağlayıcısı bu bileşenler ile ilgili hizmet sağlamıyor veya destek sunmuyorsa, güvenlik ve kullanım sorumluluğu tamamen kullanıcıya aittir (Carstensen, 2012).

Şablonlar: Bulut bilişim, sanallaştırılmış ortamda işletilecek yeni bir işletim sisteminin temelini oluşturabilmek için, bir kullanıcı tarafından geliştirilen bir taban görüntüsü olan şablon kavramını destekler. Şablonlar kuruluşun sunduğu uygulamaların sürekliliğini sağlarlar ve işletme kolaylığı için kullanışlıdırlar. Aynı zamanda yeni uygulamaları oluşturmak için iş yükünü azaltırlar. Geliştiriciler sıfırdan bir uygulama ortamı yaratmak yerine, uygun bir şablon seçip onu klonlayarak, proje üzerinde verimli bir şekilde çalışmaya başlayabilirler.

Birçok bulut sağlayıcısı şablonların daha yaygın bir biçimde paylaşılmabilmesi için açık şablonlar olarak anılan bileşenler sunar. Bu yapıda, bulut ortamındaki herhangi bir kullanıcı şablonlara erişilebilir. Bu şablonların sağlayıcıları, şablonları kendi yükleyip, yapılandırdığı ürünleriyle önceden dolduran yazılım satıcıları da olabilir. Bir yazılım satıcısının şablonunu kullanmak da kendi şablonunu oluşturmak gibi operasyonel verimliliği artırır, deneme sürümlerini teşvik eder ve uygulama satışının artmasını sağlar (Carstensen, 2012).

Açık şablonlar ile ilgili önemli bir konu, bu şablonların kasıtlı ya da kasıtsız olarak virüs, malware ve benzeri tehlikelere açık olmasıdır. Ayrıca, şablon kötü yapılandırılmışsa güvenlik ihlalleri sıkça görülebilecektir.

Lisanslama: Yazılım lisansları, yazılım bileşenlerinin kullanım koşullarını düzenlemekte olup, bu koşullara uyulması BT operasyonlarının son derece önemli bir yönüdür. Bulut bilişim ortamlarında yazılım lisanslama konusu oldukça karmaşık olabilir. Burada, ilgili yazılım bileşeninin lisans koşullarına uyulmasının sorumluluğu, yazılım bileşenini içeren kaynakları sağlamaktan sorumlu olan taraftadır. Örneğin, bulut sağlayıcı hipervizör yazılım lisanslama koşullarına uymakla sorumlu iken, bulut

kullanıcısı, kendisi tarafından yüklenen ara katman yazılımının lisans koşullarını yerine getirmekle yükümlüdür.

1.7. Bulut Bilişim Kullanım Metotları

Bulut bilişim, talebe bağlı ölçeklendirilebilir ve esnek yapısı, kullandığın kadar öde prensibiyle maliyet etkin uygulamalar sunması ve platformdan bağımsız çoklu erişim sağlaması gibi özellikleri nedeniyle onlarca uygulama alanında kendine yer bulmuş ve geleneksel bilişim mimarisinin yerini almıştır. Bulut bilişim mimarilerinin en sık kullanıldığı başlıca uygulama alanlarını aşağı gibi sıralayabiliriz:

Depolama, Senkronizasyon ve Dosya Paylaşımı: Dosya depolama, senkronizasyon ve dosya paylaşım servisleri kuşkusuz bulut bilişim mimarisinin en önde gelen kullanım yöntemidir. Dünya genelinde Google Drive, Dropbox, Box.net, Bitcasa başta olmak üzere çok sayıda dosya depolama ve paylaşım platformu bulunmaktadır. Bulut depo platformları, bireysel müşteriler tarafından kullanılabildiği gibi; kamu ve özel sektör kuruluşları da kurumsal sınıf bulut depolama mimarileri kullanarak, veri ve dosyalarını merkezileştirme yoluna gitmektedirler. Belli limitlerde ücretsiz depolama ve paylaşım olanağı sağlayan bu platformlarda, daha yüksek kotalı profesyonel kullanımlar için ölçeklendirilebilir ve talebe bağlı ücretlendirme politikası uygulanmaktadır. Sunulan hizmetlerden internet tarayıcısı olan bütün cihazlardan platform bağımsız şekilde yararlanılabilmekte olup, farklı platformlardan yüklenen dosyaların senkronizasyonu uygulama tarafından otomatik olarak yapılmaktadır. Genel olarak açık bulut şeklinde hizmet veren bu platformlar kurum ve kuruluşların ihtiyaçları doğrultusunda, kuruluşların kendi personeli için özel bulut altında da hizmet verebilmektedir. Bakanlığımız Coğrafi Bilgi Sistemleri Genel Müdürlüğü tarafından tamamlanan CBS Altyapısının Kurulması ve Geliştirilmesi İşi'nin bir alt bileşeni olan Bulut Şehir projesi, Bakanlığımız merkez ve taşra personelinin güvenli, hızlı ve platform bağımsız şekilde dosya paylaşabilmesine ve Bakanlığın veri merkezinde depoladığı dosyalarına mekân bağımsız olarak internet üzerinden güvenli bir şekilde erişebilmesine imkân tanıyan bir özel bulut uygulamasıdır. Birbiriyle entegre masaüstü, web ve mobil uygulamaların

herhangi biri üzerinden yüklenen veya paylaşılan dosyalar otomatik olarak diğer platformlarda senkronize edilmekte, çoklu paylaşım özelliği sayesinde dosyalar üzerinde ortak çalışma yapılmasına imkân tanınmakta ve üzerinde değişiklik yapılan dosyaların bütün versiyonları sistemde tutulup, gerek duyulduğunda eski versiyonlara dönüş sağlanabilmektedir. Tamamen Bakanlığımıza ait veri merkezleri üzerinden hizmet veren proje kamusal ölçekte alanında öncü projelerden biridir.

E-posta Hizmeti: Bu hizmetler yıllardır kullanılan klasik SaaS uygulamalarıdır. Gmail, Outlook, Yahoomail, Hotmail vb. gibi e-posta servis sağlayıcılarının sundukları hizmetlere internet üzerinden platform bağımsız olarak erişilebilmektedir. Birbirine entegre e-posta, takvim, belge paylaşım ve yönetimi ile masaüstü senkronizasyonu sağlayabilen uygulamalardır. Sağlayıcıların birçoğu e-posta hizmetlerini kendi özel API'leri aracılığıyla sunduklarından, kullanıcıların bir SMTP e-posta sunucusu veya servisi kurmasına veya yapılandırmasına gerek kalmadan, direkt hizmet üzerinden e-posta gönderebilmelerine imkân sağlanmaktadır.

Web Sitesi Barındırma: Bulut bilişimin en yaygın iş odaklı kullanım alanlarından birisidir. Kuruluşlar kendi web sitesi varlıklarını, bulut sunucularının yanısıra fiziksel sunucular üzerinde de barındırabilirler. Eğer bir web sitesi sadece görsel ve tanıtıcı bilgi sağlıyorsa ve depolanan veri boyutu ile işlem yükü çok fazla değişkenlik göstermiyorsa; belli kaynaklara sahip bir fiziksel sunucu üzerinde web sitesi barındırmak verimli olabilir. Ancak web tabanlı hizmetlerin sunulduğu ve işlem yükünün önemli ölçüde değişkenlik gösterdiği web sitesi uygulamalarında, kaynakların talebe bağlı büyümesi ve ölçeklendirilebilirliği olmazsa olmaz bir durum haline geleceğinden, bulut tabanlı çözümleri kullanmak en iyi seçenek olacaktır.

Felaket Kurtarma: Sunucuların üzerinde çalışan işletim sistemi, uygulamalar, yamalar ve veri gibi tüm bileşenleriyle tek bir yazılım paketine veya sanal sunucuya sığdırılabildiği sanallaştırma teknolojisi, felaket kurtarma uygulamalarına yeni yaklaşımlar getirmiştir. Artık, sanal sunucunun tümü, bir bütün halinde birkaç dakika içinde bilgisayar dışındaki bir veri merkezine kopyalanabilmekte veya

yedeklenebilmektedir. Bulut bilişim soğuk felaket kurtarma senaryoları yerine, sıcak felaket kurtarmayı mümkün kılmakta ve böylece kritik sunucuların çalışır haldeki sıcak yedekleri, paylaşılan veya özel bulut barındırma platformlarına kopyalanabilmektedir. Kopyalamanın kısa süre içinde bir bütün halinde yapılabilmesi, hem maliyet etkin ve hem de yüksek performanslı bir işlem gerçekleştirilmesine olanak sağlamaktadır. Ayrıca son yıllarda sadece sunucuların bir bütün halinde çalışır vaziyette kopyalanmasının da ötesinde, bazı bulut sağlayıcıları IP adres eşleştirmesi, güvenlik duvarı kuralları ve VLAN konfigürasyonu da dâhil bütün bir ağ yapısının kopyasını alarak, sunucuların yanında ağın da kısa sürede kurtarılmasına olanak sağlamaktadırlar.

Test ve Geliştirme Ortamı: Bulut bilişim sağlayıcıları, uygulama ve program geliştiren firmalar için kullanımı basit ve dakikalar içerisinde sanal makineler temin edip, kendi ağlarını kurup, yazılım geliştiricilerine paylaştırabilecekleri test ve geliştirme platformları sunmaktadır. Bu platformlarda geliştirilen uygulamanın farklı yükler altında nasıl çalıştığı veya farklı işletim sistemlerinde (Windows, Ubuntu vb.) ne şekilde hizmet verebildiği test edilip kıyaslanabilmektedir. Kullanılan bilişim kaynakları geliştiriciler tarafından kontrol edilebilmekte ve değişim sürekli izlenebilmektedir. Bu sayede yazılım geliştirici uygulamayı devreye aldığında farklı yüklerde ne kadar bilişim kaynağına ihtiyaç duyacağına karar verebilmektedir. Platformların sağladığı gelişmiş otomasyon, program hatalarını azaltmaya, bütünleşik yönetim uygulamasının kontrolü ile uygulamaya olan erişimi dengelemeye, kullanıma hazır yönetim araçlarının kullanım limitlerini belirlemeye ve maliyeti kontrol altında tutmaya yardımcı olur. Yine sunulan test ve geliştirme platformlarnda izleme, hata ayıklama, loglama ve güvenlik tarayıcı hizmetlerine yönelik araçlar standart olarak sunulduğundan ve bu sayede yazılım geliştiricinin bu araçları yükleyip yapılandırması gerekmediğinden; geliştirici geliştirdiği uygulamanın esas koduna odaklanabilmektedir. Kullandığın kadar öde modelinin geçerli olduğu bu platformlarda, geliştiricilerin test kodunu geliştirip test etmeleri için ek uygulama lisansları temin etmeleri gerekmez.

Kısa Vadeli Projeler: Test ve geliştirme ortamlarına benzer şekilde, bulut sağlayıcıları kısa vadeli projeler için önemli araçlar sunmaktadır. Örneğin birkaç ay kullanılacak bir

web sitesi veya mikro-site, bulut ortamında kolayca kurulup kullanılabilmekte, kullanım sonunda silinebilmekte veya daha sonra kullanılmak üzere saklanabilmektedir. Bu açıdan bulut ortamı kısa vadeli projeler için geliştirme, devreye alma ve tasarım konseptinin sınanması açısından önemli faydalar sağlamaktadır. Yine test ve geliştirme ortamında, diğer birçok bulut uygulamasında olduğu gibi, kuruluşların bilişim altyapı ve uzman personel harcamalarına sebebiyet vermeden, kullandığın kadar öde metoduyla maliyet etkin bir kullanıcı deneyimi sunmaktadır. Burada önemli olan nokta, yazılım geliştiriciler tarafından kısa bir süre için geliştirme ve test ortamı olarak kullanılan bulut kaynaklarının, projenin sürekli hale gelmesi veya boyutunun büyümesi durumlarında yetersiz kalabilmesidir. Kuruluşların test ve geliştirme için kullandıkları platformları devamlı hale getirme ve uygulamalarını bu platformlardan servis etme ihtimalini öngörüp; bulut sağlayıcı seçiminde, kendi BT politikaları ile uyumlu olma ve genişleyen veya sürekli hale gelen projeye yeterli kaynağı sağlayabilme kriterlerini göz önünde bulundurmaları gerekir.

Dönemlik Kapasite Artışı: Bulut bilişimin en önemli özelliklerinden biri ihtiyaca göre ölçeklendirilebilir yapısıdır. Yine gelişmiş bir bulut bilişim mimarisi kullanıcılarına, veritabanı sunucularını daha yüksek güvenlik seviyesine sahip bir şekilde arka planda çalıştırırken; uygulama ve web sunucularını ön planda daha esnek bir şekilde çalıştırabileceği çok katmanlı bir yapı sağlar. Bu sayede kullanıcılar sahibi oldukları uygulama ile ilgili artan talepler ölçeğinde, web ve uygulama katmanı için tedarik ettiği kaynakları artırabilir ve sonrasında talebin durumuna göre azaltabilir. Bu sayede bilişim kaynaklarının atıl kalması engellenmiş olur.

Küresel Hizmetler: Geleneksel bilişim mimarisi ile müşterilerine hizmet veren kuruluşlar, genellikle müşterilerinin yoğun olduğu bölgelere veri merkezleri kurma yolunu tercih etmektedir. Ancak sağladığı hizmet doğrultusunda küresel ölçekte erişilebilir olmayı amaçlayan kuruluşlar için bulut bilişim mimarisi yeni olanaklar getirmektedir. Birçok bulut servis sağlayıcısı günümüzde, dünya çapında dağılmış veri merkezleri ile küresel çapta bilişim kaynağı kiralama hizmeti sunmaktadır. Örneğin, Türkiye'de yerel olarak hizmet veren bir kuruluş için, aynı hizmeti Amerika Birleşik

Devletleri'ndeki potansiyel müşterilerine daha hızlı ve kesintisiz bir şekilde verebilmek amacıyla, o bölgede veri merkezi olan bir bulut servis sağlayıcısından kiralama yapmak ve iki farklı lokasyonda sunduğu hizmeti tek elden yönetebilmek akıllıca olacaktır. Bulut bilişim küresel ölçekte hizmet veren şirketlere, hedef müşterilerinin bulunduğu lokasyonlarda daha iyi içerik, ürün veya hizmet sağlayabilmek için; kolayca bilişim varlığı sahibi olma imkânı vermektedir.

Büyük Veri Uygulamaları: Büyük veri; bilimsel enstrümanlar, sensörler, internet alışverişi, email, video stream gibi çeşitli kaynaklardan gelen büyük boyutlu, çok yönlü ve dağıtık verilerdir. Günümüzde günlük ortalama 2,5 milyar gigabyte veri üretilmektedir. Yine, yapılan araştırmalar 2020 yılında yıllık 43 trilyon gigabyte veri üretileceğini ortaya koymaktadır. Çağımızda oluşan bu veri çığı, verinin kolay toplanması, ulaşılması, işlenmesi, analiz edilmesi ve anlamlı bilgi elde edilmesi için yeni modellerin, mimarilerin, programlama platformlarının geliştirilmesini gerekli kılmaktadır. Bulut bilişimin bu işlemlerin kolayca yapılması için sağladığı avantajlar nedeniyle bu iki kavram birbirinden ayrı düşünülemez hale gelmiştir. Bulut bilişimin talebe bağlı olarak dikey olarak ölçeklendirmeye imkân tanıyan mimarisi büyük veri içeren uygulamaların işletilmesini kolaylaştırmaktadır. Dikey ölçeklendirme, uygulamaların kullanımına yönelik talep artış ve patlamalarına uyum sağlayacak şekildedir. Büyük veri ortamları; büyük miktarlarda, yüksek hız ve çeşitli biçimlerdeki veriyi işleyen araçları desteklemek için sunucu kümelerine ihtiyaç duymaktadır. Bulutlar; sunucu, depolama ve ağ kaynak havuzlarına kurulmuş ve gerektiği ölçüde aşağı yukarı ölçeklendirilebilir yapılar olduğundan bu ihtiyaca cevap vermektedir. Bu anlamda bulut bilişim, büyük veri teknolojilerini desteklemek için uygun maliyetli bir yol ve gelişmiş iş analitik uygulamaları sunmaktadır.

Web ve Mobil Uygulamalar: Günümüzde hemen her gün yeni bir web sayfası veya mobil uygulama hedef kitlesine hizmet sunmak için çeşitli kuruluş ve topluluklarca devreye alınmaktadır. Bu sayfa ve mobil uygulamaların birçoğu özellikle piyasaya ilk sürüldüğü zaman bulut ortamlarında barındırılmaktadır. Bulut mimarisinde hizmet vermek, uygulamanın hedef kitlesi tarafından kabul görmemesi durumunda, uygulama

sahibi tarafından az bir zararla devre dışı bırakılabilmesine; çok yoğun şekilde kullanılması durumunda ise altyapısındaki kaynak miktarının talep ölçeğinde artırılarak kullanılabilirliğinin sürdürülmesine olanak sağlamaktadır. Bu sebeple birçok kuruluş, web sayfa ve servislerine daha fazla tüketicinin akıllı cihazlar yoluyla erişebilmesini mümkün kılmak amacıyla, çoklu erişim platformu sağlayan bulut ortamına ilgi duymaktadır.

Reklam ve İlanlar: Her gün web sayfalarında veya mobil cihazlarımızda sıkça karşılaştığımız reklamlar her ne kadar birbirinden bağımsız görünseler de, aslında merkezi platformlar tarafından yönetilmekte ve bu sayede kullanıcıların profillerine özel reklamlar cihazlarında görüntülenebilmektedir. Bulut tabanlı reklam yayınlayıcı şirketler tarafından servis edilen uygulamalar, reklamların seçilebilmesine, üzerinde işlem yapılabilmesine ve yayılabilmesine destek vermektedir. Burada reklamlarla ilgili içerik ve fiyat bilgileri, son kullanıcıların arama ve seçimleri baz alınarak ilgililerle eşleştirilmekte ve o andaki ilgi alanlarına ait reklamların gösterimi sağlanmaktadır. Büyük veri yönetimi gerektiren bu süreç, reklam şirketlerinin bilişim kaynak ihtiyaçlarını bulut sağlayıcılardan temin etmesini zorunlu kılmıştır.

Yoğun İşlemci Gücü Gerektiren Uygulamalar: Bulut bilişimin en önemli faydalarından biri yüksek performanslı işlem kaynaklarına kısa sürede erişebilme yeteneği sağlamasıdır. Büyük miktarda veri barındıran reklam, sosyal medya veya sağlık uygulamaları ancak yüksek performanslı kaynaklar kullanılarak etkin biçimde işlenebilir. Uygulamaların devreye alınması, yapılandırması ve kullanımı için geleneksel mimarilerde haftalar veya daha uzun sürebilen çalışmalar, bulut mimarisinde günler hatta saatler sürebilir. Ortaya çıkan maliyetler ise geleneksel ortamlara kıyasla çok cüzidir.

Finansal Hizmetler ve E-Ticaret: Günümüzde birçok şirket, ürünlerini ve hizmetlerini internet üzerinden pazarlamak için online alış veriş siteleri hizmete sunmaktadır. Yine birçok şirket ve tüketici finansal işlemlerini yapmak için internet bankacılığı platformlarını kullanmaktadır. Çok fazla veri üretilen, yığılan ve veri miktarı sürekli

artan bu hizmetlerin kullanılabilirliğinin devamı için, bulut bilişim ölçeklendirilebilir bir altyapı sunmaktadır. Bu hizmetlerin en önemli ortak özelliği, müşterilere ait kişisel verileri barındırmaları ve bu sebeple de kişisel veri güvenliği ile ilgili ek bilgi güvenliği önlemleri gerektirmeleridir. Günümüzde bu uygulamaların kuruluşların geleneksel mimarideki veri merkezleri yerine özel bulut veya kişisel verilerin bulutun müşterilere açık kısmından ek güvenlik duvarlarıyla izole edilip korunduğu, hibrit bulut mimarileri üzerinde hizmet vermesi daha güvenli hale gelmiştir.

1.8. Bulut Bilişimin Getirdiği Avantajlar ve Riskler

Kendinden önceki bilişim teknolojilerinin mimarisine uygun özelliklerini bir araya getirerek bir iş modeli oluşturan bir teknoloji olarak bulut bilişim, farklı önem derecesine sahip onlarca avantajının yanında, birçok riski de yapısında barındırmaktadır. Bu bölümde bulut bilişim mimarilerinin kullanımının kullanıcılara getirdiği, genel kabul görmüş başlıca avantajlara ve risklere kısaca yer verilecektir. Bulut bilişimin kamu alanında kullanımının getireceği avantaj ve faydalara ikinci bölümde geniş kapsamlı olarak değinilmekte olup, risklerle ilgili detaylı analizler ise üç ve dördüncü bölümlerde yer almaktadır.

1.8.1. Avantajlar

Düşük Maliyet: Bulut bilişim kullanımını yaygınlaşmasının hiç şüphesiz en önemli nedeni getirdiği maliyet avantajlarıdır. Burada maliyet avantajı hem kullanıcı hem de sağlayıcı açısından ortaya çıkmaktadır. Kullanıcılar uygulamalarını geliştirmek, çalıştırmak ve verilerini barındırmak için pahalı bilişim donanım ve yazılımlarına ihtiyaç duymadan, bütün bu işlemleri web tarayıcı olan cihazlar üzerinden yönetebilmektedirler. Bütün işlemler bulut tarafındaki sunucularda yapılıp, ilgili veri merkezlerindeki depolama ünitelerinde barındırıldığından, kullanıcının sahip olduğu sistemin performansının hizmete etkisi azalmaktadır. Diğer bir avantaj ise uygulamalar ve sistemin idamesi için bulundurulması gereken uzman insan kaynağı sayısının ve dolayısıyla personel maliyetinin geleneksel mimariye oranla önemli ölçüde düşmesidir.

Sağlayıcı açısında ise, sanallaştırma sayesinde aynı fiziksel donanım üzerinden çok sayıda kullanıcıya hizmet verilebilinmesi ve sağlayıcının talep edilen kaynak miktarına göre hizmet sunumunu optimize edip, atıl kaynaklarını asgari düzeye indirebilmesi ciddi maliyet avantajı sağlar. Bulundurulan altyapı ne kadar büyük olursa, birim işlem başına donanım, yazılım, enerji, uzman personel vb. maliyetler bir o kadar düşecek ve karlılık artacaktır. Dünyanın farklı ülkelerinde bilişim kaynaklarından faydalanma saatleri farklılık göstermektedir. Örneğin Japonyada kaynak talebinin pik yaptığı bir anda Avrupa'daki talep asgari düzeydedir. Bu durum özellikle küresel sağlayıcılara bulutun esnek ve ölçeklendirilebilir yapısı sayesinde aynı kaynağı farklı lokasyonlardaki müşterilerine farklı zaman dilimlerinde farklı oranlarda sunma imkânı sağlar. Ayrıca diğer bir avantaj ise, sağlayıcıların veri merkezlerini istedikleri lokasyonlarda kurabilmeleri esnekliği sayesinde, düşük kira ve enerji gideri olan lokasyonlarda veri merkezlerinin kurulabilmesidir.

Erişilebilirlik: Bulut bilişimin diğer bir önemli avantajı sağladığı erişim kolaylığıdır. İnternet üzerinden erişilebilir altyapısı sayesinde, sistem yönetim araçlarına, uygulamalara ve verilere her ortamdan kolayca erişim sağlanabilmektedir. Ayrıca en ciddi bulut hizmetlerinin bile mobil uygulamalar sunduğu günümüzde, erişim eldeki cihaz ile sınırlı değildir. Sonuç olarak, işletmeler çalışanlarına daha esnek çalışma saatleri sunabilir ve kendilerine uygun bir iş-yaşam dengesi oluşturmalarına imkân tanıyarak, üretkenliği düşürmeden memnuniyetlerini artırabilir (Salesforce, 2015).

Grup Çalışması ve Uygulama Test Kolaylığı: Bulut bilişimin en büyük avantajlarından biri de aynı belge üzerinde aynı anda birden çok kişinin düzenleme yapabilmesidir. Örneğin, Google Docs'un hesap tablosu uygulaması aynı belge üzerinde aynı anda birden çok kişinin çalışmasına imkân vermektedir. Bunun yanında, dosyalar kişisel bilgisayarlar yerine bulutta depolandığı için kullanıcılar, internet bağlantısına sahip olan herhangi bir bilgisayar ile belgenin en güncel haline her an ulaşabilmektedir (Çintimur, 2014).

Aynı şekilde bulut bilişim, uygulama yazılımlarının devreye alınmasından önce yapılacak testler için, geleneksel mimarilere göre daha uygun bir mimaridir. İşletmelerin testleri için ayrı bir test sunucusu temin etme ihtiyaçları ortadan kalkar. Sanal olarak ayrılan test sunucusu üzerine birebir yedeği yüklenen uygulama yazılımı, dağıtık ortamda birçok kullanıcı tarafından aynı anda test edilebilir. Yine bu sayede uygulamalar üzerinde penetrasyon ve özellikle de yük testleri kolayca yapılabilmektedir.

Esneklik: Bulut tabanlı servisler, sürekli büyüyen veya dalgalı bant genişliği talebi olan işletmeler için idealdir. İhtiyaç arttığında, uzak sunucular üzerindeki kaynak kapasitesi kolayca artırılabilir. Aynı şekilde tekrar kaynağın azaltılması gerektiğinde servis buna uyumludur. Sistemin bu çevikliği kullanıcı işletmelere, rakiplerine göre gerçek bir avantaj sağlar ve bu sebeple BT yöneticileri ve CIO'lar operasyonel çevikliği buluta geçiş için başlıca etmen olarak görmektedirler (Salesforce, 2015).

Bulut bilişimin önemli bir karakteristik özelliği, hizmet alıcılara kaynakların sınırsız olduğu izlenimi vermesidir. Geleneksel sunucu altyapıları, istemcilerden gelen işlem taleplerinin kısa sürede birkaç katına çıkması durumunda, bu taleplere cevap veremezler. Ancak bulut bilişim mimarisi esnek bir şekilde ilgili sanal sunucunun kullandığı bilişim kaynağını artırarak iş ve veri kaybının önüne geçebilir.

Gelişmiş Performans: Bulut uygulamaları, kullanıcı erişim platformunda, bu platformlarda yüklü uygulamalara göre çok daha az sistem kaynağı tükettiği için, sistemlerde herhangi bir performans kaybı yaşanmaz. İşlemin ve depolamanın büyük çoğunluğu sağlayıcı tarafında yapıldığı için, çoğu uygulama için cep telefonlarının düşük bilişim kaynakları dahi yeterlidir. Ayrıca bulut bilişimde çok yoğun işlemci gücü gerektiren test-geliştirme veya büyük veri uygulamaları, ilgili iş yükü için gerekli kaynak artırılarak ve fiziksel olarak farklı lokasyonda bulunan kaynaklar bir iş için birleştirilerek kısa sürelerde tamamlanabilir.

Yazılım Yükleme ve Güncelleme: Bulut bilişimde ve özellikle de SaaS servislerinde, sağlayıcı çoklu kullanıcılarına hizmet aldıkları uygulamaları çalıştırabilmek için sanal sunucular ve depolama üniteleri tanımlar. Burada bu sunuculara işletim sistemi,

güvenlik ve performans artırma yazılımları, uygulamaların çalışması için gerekli destek yazılımları ve diğer uygulama arayüz yazılımlarının yüklenmesi tamamen sağlayıcının sorumluluğunda olup; sağlayıcı bu yazılımları kendi yönetim panelinden kolayca çoklu olarak kurup kaldırabilir, yedekleyebilir, fiziksel sunucuların bakım ve arıza zamanlarında diğer sunuculara taşıyabilir. Bütün bu işlemler geleneksel mimarilere oranla çok daha kısa duruş zamanlarında tamamlanabilir. Yine verilerin farklı lokasyonlara, idealde sınırsız boyutta ve istenilen formatta yedeklenebilmesi, felaket kurtarma sistemlerinin işletilmesini kolaylaştırmaktadır.

Yine özellikle SaaS servis sağlayıcıları, servis ettikleri uygulamalarının çalışabilmesi için gerekli yazılımların son sürümlerini, piyasaya sürüldükten çok kısa bir süre sonra müşterilerine sunabilmektedirler. Çalışanları daha verimli hale getirebilmek için, yeni özellikler ve işlevler, sürüm yükseltmeleri ile ivedilikle temin edilmektedir. Ayrıca, yazılım geliştirmeleri oldukça sık yayımlanmaktadır. Bu durum, yılda sadece bir kez yeni sürümü yayınlanan ve bu sürümlerin piyasaya yayılması önemli bir zaman alan ticari amaçlı yazılımların aksine, büyük zaman ve iş tasarrufu sağlamaktadır (Coles, 2015).

Sistem İzleme, Ölçme ve Raporlama: Az sayıda uygulama işletmesi gereken olan kuruluşların 24/7 altyapılarını izlemeleri zaman alıcı ve pahalıdır. Dışarıdan yönetilen bir bulut çözümünde bu iş sağlayıcı tarafından kullanıcı adına yapılmaktadır. Sistemin izlenmesi ve verilerin güvenli bir şekilde depolanmasının yanında, sağlayıcılar kullanıcı ihtiyaçları doğrultusunda yaratıcı ve pratik çözümler üretirler. Ayrıca verimli çalışan BT altyapılarını korumak için kullanıcılarına uzman, duyarlı ve iş odaklı tavsiyeler sunarlar (Rackscape, 2016).

Bulut bilişimde esnek bir ölçeklendirilebilirlik olması; izleme, ölçme ve raporlama işlemlerini önemli hale getirmektedir. Servis edilen uygulamanın kullanılabilir biçimde çalışması için ihtiyacı olan bilişim kaynakları, yapılan ölçüm sonuçlarına göre artırılıp azaltılabilmekte ve zamanla değişen ihtiyaçlara göre yeniden optimize edilebilmektedir. Günümüzde birçok SaaS ve Paas servisi kaynak

optimizasyonunu, uygulamaların zamanla değişen ihtiyaçlarına göre otomatik olarak yapabilme kabiliyetini kazanmıştır. Ayrıca bulut mimarilerinde sağlanan gelişmiş raporlama arayüzleri, dönemlik performans değerlerine bağlı kullanım miktarlarının kaydını tutmaları yanında, ileride uygulamalara yapılacak eklentiler ve geliştirilecek benzer uygulamalar için kaynak teşkil etmektedirler.

Artırılmış Güvenlik ve Uyum: İş ile ilgili gelir ve itibar kaybına uğramaktan korunmak ve sıkı yasal yükümlülükleri yönetmek her zaman ön planda tutulması gereken konulardır. Bulut ortamı bu konulardaki sorumluluk yükünü önemli ölçüde kullanıcıların omuzlarından alır. Bulut sağlayıcı, kullanıcı için altyapı düzeyinde esnek ve çevik bir platform inşa edecek ve kullanıcıya uyum ve düzenleyici gereksinimleriyle başa çıkma konusunda yardımcı olacaktır (Rackscape, 2016).

Bulut bilişimde uygulamalar, API'ler ve depolanan veriler internete bağlı yedeklenmiş veri merkezlerinde tutulduğundan, kullanıcının kişisel cihazında yaşanacak herhangi bir güvenlik açığı; veri merkezindeki kaynakları koruyan güvenlik duvarları aşılmadan veri kaybına yol açmaz. Ayrıca genel olarak bulut sunucularında her verinin bir kopyası otomatik olarak başka bir sunucuya da kopyalanır. Bulut hizmeti sağlayıcıları en yüksek güvenlik seviyelerine sahip veri merkezlerini kurar veya kiralarlar.

Uyum sorunu geleneksel mimarilerde çokça yaşanmaktadır. Örneğin Windows yüklü bir bilgisayar ile Mac veya GNU/Linux yüklü bir bilgisayar arasında ağ bağlantısı kurmak ve aynı uygulama üzerinde çalışmak oldukça zordur. Bulut bilişimde veriler sunucuda bulunduğu için herhangi bir işletim sistemiyle bu dosyalara sorunsuz bir şekilde ulaşılabilir.

1.8.2. Riskler

İnternet Bağlantısı ve Bant Genişliği: Bulut bilişim ortamında iş sürekliliğini etkileyen önemli bir risk internet bağlantısı kaybıdır. Bu sebeple internet bağlantısının asgari düzeyde kesintiye uğraması konusunda sağlayıcının ne gibi tedbirler aldığının açıklığa

kavuşturulması gerekir. Örneğin, bir güvenlik açığı tespit edilmesi halinde, güvenlik açığı giderilene kadar bulut sağlayıcı ile tüm erişimi sonlandırmak gerekebilir. Ek olarak, kolluk kuvvetleri tarafından bir veri barındırma sunucusuna el konulması durumunda; aynı makinede kayıtlı olan diğer hizmetler de, konu ile ilgileri olmasa da kesintiye uğrayabilirler (Ulrey, 2014).

Bulut bilişimin sürekliliği için internet bağlantısıyla ilgili diğer bir risk de geniş bant altyapısıdır. Geniş bant altyapılarının veri aktarım taleplerine cevap vermekte zorlandığı günümüzde; internet üzerindeki veri aktarım hızı, yerel ağ bağlantılarındaki veri aktarım hızına oranla çok düşük kalmakta ve bu durum internet bağlantısının vazgeçilmez olduğu bulut mimarilerinin kullanıma yönelik bir risk unsuru olarak karşımıza çıkmaktadır. 4G ve 5G teknolojilerinin yaygınlaşmasıyla birlikte bu durumun büyük oranda geçerliliğini yitireceği düşünülse de, bulut bilişim için hala büyük bir dezavantajdır.

Veri Mahremiyeti ve Veri Güvenliği: Kişiye özel ve gizli verilerini bulutta barındıran kuruluşlar, veri güvenliği kontrolünü önemli miktarda sağlaycılara aktarmış olurlar. Bu nedenle sağlayıcının, kuruluşun veri gizliliği ve güvenliğine ilişkin ihtiyaçlarını kavradığından emin olmak gerekir. Yine sağlayıcının, kuruluşun bulunduğu ülkede hukuki olarak geçerli olan, veri güvenliği ve gizliliği ile ilgili kural ve düzenlemelerin farkında olduğundan emin olmak gerekir (Romes, 2013).

Bulut hizmeti alan kuruluş, gelecekte kişisel veya gizli verilerinin ifşa olması veya sızması ile ilgili hukuki bir sorun yaşamak istemiyorsa; ülkesinde veri mahremiyeti ve gizliliğine ilişkin geçerli olan mevzuata uygun şekilde hizmet seviye anlaşmaları (SLA) imzalayarak, sağlayıcıya bu konuda sorumluluk yüklemelidir. Bu sözleşmelerde sağlaycının sorumlulukları ve hizmet alan kuruluşun yükümlülükleri açıkça belirtilmelidir.

Sistem Güvenliği: Çok fazla sayıda kullanıcı ve bilişim kaynağının olduğu bir ortamda sistem güvenliği riskleri kaçınılmazdır. Bulut ortamları genellikle bot, virüs, kaba kuvvet saldırılarına ve diğer saldırılara uğrarlar. Burada kullanıcıların erişim kontrollerinin,

güvenlik açığı değerlendirme uygulamalarının, yama ve yapılandırma yönetimi kontrollerinin; verilerinin korunması için yeterli düzeyde olması önemlidir. Bu sebeple, verileri bir dış kaynak olarak sağlayıcıyla paylaşmadan önce, verilerin nasıl güvenle korunacağı ve saklanacağına ilişkin şartlar hizmet seviye anlaşmasında açıkça belirtilmeli ve bu şartlar yönetim ve güvenlik risklerini azaltmayı hedeflemelidir. Yine burada gerektiğinde korunmalarını sağlamak üzere, verilere ve ilgili güvenlik önlemlerine hangi kişilerin erişim sağlayacağı açıkça belirtilmelidir.

Güvenilirlik ve Veri Yönetimi: Bulut müşterilerinin ve özellikle de uygulamalarını bulut üzerinden servis edenlerin, itibar ve gelirlerini koruma adına, hizmet kesintilerine tahammülleri yoktur. Bu sebeple sık yaşanabilecek kesinti durumlarına karşı hizmet seviye anlaşmalarında gerekli önlemler alınmalıdır. Ayrıca birçok bulut müşterisi verisinin hangi lokasyonda depolandığını bilememekte ve birçok sözleşmede sağlayıcının verilerin tutulması için hizmet aldığı alt yüklenicilerden bahsedilmemektedir. Bu durum uzun vadede verinin kontrolü ve yönetimi ile ilgili riskler barındırmaktadır.

Güvenilirlik ile ilgili bir diğer konu da, hizmet sağlayıcısı firmaların gerekli alt yapı, yeterli sermaye, asgari uzman personel vb. kriterlere ilişkin herhangi bir izin ya da yeterlilik ön şartı bulunmamasıdır. Bu konuda herhangi bir yasal düzenleme ve denetim olmaması ve üyelik işlemleri sanal ortamda yapılması gibi sebeplerle; hizmet alan kullanıcılar, hizmete son verilmesi durumunda, veri kaybı, kişisel verilerin ifşası vb. konularda mağdur olabilmektedirler.

Ayrıca bulut bilişim mimarilerinde güvenlik, kullanılabilirlik, veri gizililiğinin sağlanması vb. konularda belirli standartların uygulanması, düzenli olarak denetlenmesi ve bu standartlara göre hizmet sunan sağlayıcı kuruluşların yeterliliklerinin belgelendirilmesi gerekmektedir. Böylece kullanıcılar tercihlerini yaparken, bilgilerinin güvenliğinin sağlanıp sağlanmayacağı konusunda, hizmet sağlayıcılara yeterlilik sertifikasını veren kuruluşları göz önüne alabileceklerdir.

Mevzuat ve Standartlar: Bulut bilişim mimarisi yapısı gereği küresel ölçekte hizmet verme kabiliyetine sahip bir teknolojidir. Ancak her bir ülkenin bu teknoloji ile ilgili mevzuatları birbirinden farklı, yetersiz veya uyumsuz olabilmektedir. Örneğin Avrupa Birliği'nin verilerin korunması hakkındaki direktifine (EU Data Protection Directive) göre, bulut bilişim hizmeti verecek olan firmaların Avrupa Birliği ülkeleri dışında kuracakları veya Avrupa Birliği dışından kiralayacakları sunucu hizmetlerinde; sunucuların bulunduğu ilgili ülkelerin Avrupa Birliği yasalarının belirlemiş olduğu veri koruma güvenlik seviyesinde olması gerekmektedir. Ancak Amerika Birleşik Devletleri de dâhil hemen hiçbir ülke bu standartlara uymamaktadır. Ancak sunucu sahiplerinin dünyanın çeşitli noktalarında konumlanmış olmaları ve farklı mevzuat uygulamalarına tabi olmaları önemli riskler yaratmaktadır.

Aynı şekilde bulut sağlayıcıları arasında da, bulut hizmetleri açısından ortak standartlar geliştirilmesi konusunda fazlaca yol alınamamıştır. Sağlayıcılar hizmetlerinden tam olarak memnun olmayan müşterilerini kaybetme ve artan rekabet ortamında hizmet ücretlerinin düşerek karlarının azalması ihtimallerini göz önünde bulundurarak, standartlaşmaya karşı durmaktadırlar. Ancak istenildiği takdirde hizmetlerin bir sağlayıcıdan diğerine aktarılabilmesi veya aynı hizmet için eş zamanlı iki farklı sağlayıcının hizmetinin kullanılabilmesi müşterilerin önde gelen taleplerindendir.

Hizmet Sağlayıcıların Lehine Hizmet Sözleşmeleri: Bulut hizmet sağlayıcılar, kullanıcı ile yapmış oldukları sözleşmelerde; bilgi güvenliğinin sağlanması ve veri bütünlüğünün korunmasına ilişkin tüm sorumluluğun kullanıcıya ait olduğunu ve hizmetin kullanımı ile bu şartın kabul edilmiş olduğunu belirtmektedirler (Microsoft, 2016). Bu tür hizmet sözleşmeleri karşısında kullanıcı haklarını koruyan yasal düzenlemeler olmaması nedeniyle, bulut sistemi üzerine aktarılan verilerin kaybolma riskinin, kullanıcı tarafından göze alınabilir nitelikte olması gerekmektedir.

Bulut hizmet sağlayıcılar, hizmetlerde meydana gelen kesintiler ya da hizmet sağlayıcı tarafından hizmetin herhangi bir sebep gösterilmeksizin sonlandırılması

durumunda, meydana gelebilecek kayıplar ve bulut mimarisi üzerinde bulunan bilgilerin iade edilmesi konusunda sorumluluk almamaktadırlar (Microsoft, 2016).

Ayrıca bulut bilişimde sağlayıcı tarafından sunulan hizmetlerin düzeyi konusunda, her ne kadar kaynaklara ilişkin ölçümler yapılabiliyor olsa da, irade çoğunlukla sağlayıcı tarafında olup; hizmet kalitesinin sözleşmede belirtilen düzeyde sağlanıp sağlanamadığının takibi kolay değildir. Özellikle kısa süreli hizmet kesintisi vakalarının tespiti ve sağlayıcı önünde ispatı konusunda kullanıcının genelde yeterli kabiliyeti yoktur.

1.9. Bulut Bilişim SWOT Analizi

BT hizmetlerinde bulut bilişimin mimarisinin kullanımının, kurum ve kuruluşlar açısından çeşitli güçlü ve zayıf yönleri ile ortaya çıkardığı fırsat ve tehditler bulunmaktadır. Bu bölümde kurumsal kullanım için bulut bilişim mimarisi, kendinden önceki geleneksel bilişim teknolojileriyle kıyaslanacak ve aradaki farklar göz önünde bulundurularak bir SWOT analizi yapılarak, bu teknolojinin kullanımının olumlu ya da olumsuz iç ve dış faktörleri tanımlanacaktır. Burada güçlü yönler bulut bilişimin genel kabul gören temel değerlerini, fırsatlar ise bulut bilişimin geleceğini şekillendirecek olan, sürdürülebilir ve kazançlı bir iş modeli oluşturulmasını sağlayacak faktörleri tanımlar. Zayıf yönler bulut bilişimin daha etkin kullanılabilmesi için kendinden önceki bilişim teknolojilerine kıyasla güçlendirilmesi gereken, tehditler ise bu teknolojinin kullanım sürecinde aksamalara neden olma riskini barındıran faktörleri tanımlamaktadır.

Güçlü Yönler: Bulut bilişim mimarisinin kurum ve kuruluşlar açısından öne çıkan en önemli yönlerinden biri sağladığı maliyet tasarrufudur. Günümüzde birçok kamu ve özel sektör kuruluşu temel görevlerinin ve iç iş süreçlerinin yanısıra, internet vasıtasıyla vatandaşlara çeşitli hizmetler sunmak amacıyla bilişim kaynaklarını kullanmaktadır. Hizmetlerini internet yoluyla sunmak kuruluşlara daha az personel çalıştırma, daha az ve küçük ofis ve şubelerde hizmet verebilme ve hizmeti hızlı, her yerden erişilebilecek şekilde sunma gibi birçok avantajlar sağlamaktadır. Buradaki maliyet avantajının üstüne, bir de bulut bilişimin getirdiği kaynak kiralama yönteminin; geliştirilen uygulama için

altyapı (donanım ve yazılım) yatırım, bakım ve güncelleme maliyeti ile uzman bilişim personeli ihtiyacını asgari seviyeye indirmesi, kuruluşlara ciddi maliyet avantajı sağlar.

Donanım altyapısının idamesinin yanısıra; uygulamaların güvenliği, kullanılabilirliği ve erişilebilirliğinin artırılmasına yönelik tüm yazılım paket, eklenti ve yamaların kurulumu ve ayrıca her türlü yazılım uyumsuzluklarının giderilmesi sağlayıcının sorumluluğunda olup, bu işler için uzman BT personelinin istihdamı ve ek lisans temini ihtiyaçları ortadan kalkar. Sağlayıcı platformları, talebe göre müşterilerine bakım, izleme, yönetim ve güvenlik kontrolleri gibi konularda geniş hizmetler sunabilir.

Esneklik ve ölçeklendirilebilirlik özellikleri sayesinde bulut bilişim kullanıcıları sabit ücret politikasından kurtularak, zamanla değişen kaynak ihtiyaçlarına göre anlık ihtiyaç duydukları kaynakları talep ve temin ederler. Ücretlendirmenin tamamen kullanım bazlı olması, kullanılmayan kaynağın ücretinin ödenmesi durumunu ortadan kaldırır. Ayrıca son yıllarda standartlaşmanın artmasıyla birlikte, bulut bilişim kullanıcılara, sağlayıcılar arasında geçiş esnekliği de tanımakta ve bu sayede kullanıcılar değişen ücret politikalarına göre servis sağlayıcılarını, hizmet seviye anlaşmalarına (SLA) aykırı olmayacak şekilde değiştirebilmektedir.

Sağlayıcılar, müşterilerinin değişen ihtiyaçlarını karşılayacak şekilde kaynak bulundurmakla yükümlü olup, bir müşterisinin kaynak talebi azaldığında bulundurdukları bu kaynağın atıl durumda kalmaması için, kaynaklarını mümkün olduğunca çok müşteri ile paylaştırırlar. Bu sayede bazı müşterilerinin azalan talebi sebebiyle boşa çıkan fazla kaynağı, talebi artan diğer müşterilerine aktararak kaynaklarının atıl kalmasını minimize etmeye çalışırlar. Kaynakların mümkün olduğunca etkin kullanılması durumu dolaylı olarak birim kaynak kiralama ücretlerini azaltacağından müşteri için de avantaj sağlar.

Bulut bilişimin diğer bir güçlü yönü, internet bağlantısı olan herhangi bir lokasyondan sanal erişim imkânı sağlamasıdır. Erişimin lokasyon ve platform bağımsız olması, kuruluşlara kendi veri merkezlerine bağlı kalmadan farklı bölgelerde satın

aldıkları veya kiraladıkları kaynaklar vasıtasıyla, hizmetlerini hedef kitlelerine sunma kabiliyeti sağlar.

Fırsatlar: Bulut bilişim mimarisi, geleneksel bilişim mimarilerinin hizmetlerini sağlayabildiği gibi, müşterileri için yeni çözümler üretmektedir. Ancak bulut ortamında sunulan hizmete ilişkin belirleyici faktör müşteri talebidir. Müşterinin talebi karşılandığı sürece, bulut bilişim mimarisi geleneksel bilişim mimarilerinin çözümlerini aynı düzeyde sunmak zorunda değildir. Örneğin, müşteri kuruluşlar sadece kritik ve gizli içeriğe sahip olmayan veri yığınını bulutta barındırabileceği gibi, ticari öneme sahip ve herhangi bir şekilde kesintiye uğraması itibar kaybı yaratabilecek bir uygulamasını da bulut üzerinden servis edebilir. Burada sağlayıcı müşterinin beklentileri doğrultusunda altyapısını kuracak ve ücretlendirmeyi de buna göre hesaplayacaktır. Başka bir deyişle sağlayıcılar farklı müşteri taleplerine göre farklı iş modelleri oluşturacak, buna göre hizmet seviye anlaşması düzenleyecek ve bu doğrultuda hizmetini sunacaktır. Bulut bilişimin esnek yapısı bu noktada sağlayıcıya, müşteri talepleri doğrultusunda çok fazla sayıda iş modeli oluşturabilme, müşteriye ise sadece talebi doğrultusunda hizmet alıp, ihtiyacı olmayan ve kullanmayacağı araç ve çözümlere ekstra ücret ödemekten kaçınma fırsatı sunmaktadır.

Bulut bilişimde atıl durumda çalışan kaynak oranı, geleneksel mimariye göre düşüktür. Örneğin, bir uygulama için ayrılmış işlemci veya depolama ünitesi kaynakları, sanallaştırma sayesinde hizmetin kullanılabilirliğini etkilemeyecek ölçüde asgari seviyede tutulur. Bu sayede bilişim kaynaklarının ve dolayısıyla bilişim kaynaklarının çalışması için gerekli enerjinin daha verimli kullanılması sağlanır. Bu durum kullanıcı ve sağlayıcılar için çevreye duyarlı yeşil BT kullanma fırsatı oluşturur.

Yenilikçi bir teknoloji olarak bulut bilişim, geleneksel BT mimarilerine getirdiği ilerlemeler ile birlikte, bu teknolojilere oranla daha karmaşık bir yapıya dönüşmüştür. Özellikle açık ve hibrit bulut mimarilerinde, uygulamaların farklı lokasyonlardaki birçok veri merkezinde bulunan bilişim kaynakları üzerinden servis edilebildiği, kaynak ve uygulama yönetiminin çeşitli yazılımlarla sağlanabildiği, izleme, hata ayıklama, loglama

ve güvenlik tarayıcı hizmetlerine yönelik araçların sunulabildiği karmaşık bilişim mimarileri ortaya çıkar. Kullanıcılar bütün bu bileşenlerin herbiri için nitelikli uzman personel bulunduramaz ve bu amaca yönelik dış kaynaklara yönelirler. Bulut mimarisi kullanıcılarına, önemli bir kısmı bulut sağlayıcı tarafından karşılanabilecek bu ihtiyaçlara yönelik önemli fırsatlar sunar. Yine bulut bilişim, günümüzün bilişim hizmetlerine yönelik teknolojik ve ekonomik gereksinimlerini karşılamak için mevcut teknolojileri birleştiren bir iş modelidir. Bu sebeple kullanıcı kuruluşlar zaten bu teknolojilere aşinadırlar. Bu noktada mevcut teknolojilerin karmaşık bir bileşimi olan bulut bilişim kullanıcılarına, aşina oldukları teknoljileri bir arada kullanarak, kendilerine özgü iş modelleri oluşturma fırsatı sunar.

Bulut bilişimin yarattığı belki de en önemli fırsatlardan biri de ölçeği ne olursa olsun (tekil kullanıcılardan küresel ölçekli kuruluşlara kadar), bütün müşterilerine sahip olduğu farklı fonksiyonları sunarak yeni pazarlar oluşturmasıdır. Pahalı bilişim teknolojisi altyapıları, bu sayede ödeme gücü oranında bütün ihtiyaç sahiplerine ulaştırılmakta ve hatta beklentileri düşük ve bilişim kaynak talebi az olan küçük ölçekli işletmelere daha kolay sunulabilmektedir. Küçük işletmelerin bulut mimarilerini kullanma konusunda yakaladıkları başarı ve karlılık, büyük ölçekli kuruluşlarını bulut teknolojilerine entegre olmaya ve gerek açık, gerekse de özel bulut teknolojilerinin avantajlarından yararlanmaya itmiştir.

Zayıf Yönler: Bulut bilişim mimarisinin en zayıf yönlerinden biri, kullanıcıların karşı karşıya kaldığı kontrol kaybıdır. Özellikle açık bulutlarda, hizmetlerini dışarıya aktaran kullanıcılar; fonksiyonellik, tasarım, güvenilirlik, güvenlik ve diğer yönetim süreçleri üzerinde karar verebilme yeteneğini bir ölçüde kaybederler. Müşteri genellikle verilerinin depolandığı ünitenin yerini bilmez ve genellikle kendisine bu verilerin sabit bir depolama ünitesinde barındırılacağına dair garanti verilmez. Kontrol kaybının tam olarak önlenmesi zor ve yüksek maliyetli olsa da; gelecekte daha şeffaf iş modelleri sunma hedefi taşıyan sağlayıcıların, verilerin saklandığı yere ve sistemin çalışma prensibine dair bilgi vermesi mümkündür. Günümüzde Amazon gibi sektörün öncüsü

sağlayıcılar, talep eden büyük ölçekli müşterilerine yönelik, izole edilmiş sunuculara erişme olanakları sunmaktadırlar.

Günümüzde hala çoğu bulut hizmeti birlikte çalışabilirliğe uyumlu değildir. Farklı iki bulut hizmeti arasında entegrasyonu zorlaştıran bu durum sağlayıcıya bağımlılık sorununu ortaya çıkarmaktadır. Müşterilerin, hizmet sağlayıcılarını değiştirmek istemesi durumunda, veri kayıpları oluşabilir veya transfer hiç gerçekleştirilemeyebilir. Teknolojik olarak üstesinden gelinebilecek bu durumu ortadan kaldırma konusunda sağlayıcılar, müşterilerinin kendilerine bağımlı ve bu sebeple de sadık kalması düşüncesiyle, çok da istekli görünmemektedir. Ancak bulut bilişim için ciddi bir zayıflık olan bu eksiklik, müşterilerin hizmet sağlayıcısı değişikliklerini engeller ve onları özel bulutlar oluşturmaya yönlendirir. Uzun vadede artan rekabetin sağlayıcıları, daha açık ve birlikte çalışabilir sistemlere sahip olmaya doğru stratejik hamleler yaparak, tüketici segmentlerini büyütmeye ve yeni bir pazarlar oluşturmaya zorlayacağı açıktır.

Bilişim teknolojilerinde güvenilirlik, olası hizmet kesintilerinin asgari düzeyde olması veya hiç yaşanmaması, barındırılan veri ve işlem yükünde kayıpların yaşanmaması ve sunulan hizmetlere kötü niyetli kişilerce müdahale edilememesi gibi unsurlara bağlıdır. Bulut mimarileri her ne kadar ileri güvenilirlik seviyelerine sahip olsalar da, bu durum önemli bir zayıf yön olmaya devam etmektedir. Sağlayıcılar, sundukları hizmetin saygınlık, güvenilirlik ve güvenliğini iyileştirmek için çalışmaktadırlar ancak başa çıkamadıkları doğal afetler veya insan hatası gibi bazı faktörler de mevcuttur. Birçok kuruluşun hizmet kesintilerine çok fazla tahammülü olmaması nedeniyle, sağlayıcılar sistemlerinin, kesintileri önlemek amacıyla nasıl bir tasarıma sahip olduğunu ve olası bir kesinti durumunda, mümkün olduğunca hızlı bir şekilde uygulama ve verileri kurtarmak için nasıl tepki vereceğini, müşterilerine açıklamak ve kabul ettirmek zorundadırlar.

Bulut bilişim servislerinin diğer bir zayıf yönü, küresel çapta hizmetler sunabilme yeteneklerine bağlı olarak, küresel ekonomik gelişmelere karşı aşırı duyarlı

olmalarıdır. Küresel çapta yaşanan krizlerde birçok lokasyonda kısa bir zaman diliminde yaşanan talep düşüşü, yatırım yaptıkları kaynaklarının bir kısmının atıl duruma düşmesine sebep olarak ve gelir-gider dengelerini bozarak, hizmet sağlayıcıları zor durumda bırakabilmektedir.

Tehditler: Bulut bilişim mimarisinin hizmet modeli oluşturma amacıyla geliştirilmesi durumu, hizmette aksamalara yol açabilecek tehditler konusunda özel çalışılması ve önlem alınması gereksinimlerini ortaya çıkarır.

Bulut bilişim piyasası yeni gelişen bir piyasa olmasına rağmen, piyasa içindeki rekabet yüksektir. Yenilikçi ve gelişime açık teknoloji ve hizmet çözümleri, halen piyasayı domine eden sağlayıcıları, yenilikler doğrultusunda hareket etme ve kendi iş modellerini gelişmelere adapte etmeye sevk etmektedir. Geleneksel bilişim sistem üreticileri ise, yeni pazar alanları oluşturmak ve mevcut müşterilerini koruyabilmek amacıyla bulut mimarilerine geçiş yapmaktadırlar. Bulut bilişimin yapısı gereği, elinde çok fazla bilişim kaynağı bulunduran büyük sağlayıcılar ile fiyat rekabeti yapmak çok zordur. Dünyanın farklı bölgelerinde çok büyük veri merkezlerinde, merkez başına çok fazla sayıda sunucu ve depolama ünitesi bulunduran ve bu kaynaklarını kullanan onbinlerce müşteriye sahip bir sağlayıcı ile piyasaya yeni giriş yapan bir kuruluşun aynı hizmet için aynı fiyatlandırmayı yapıp aynı oranda kar etmesi imkânsızdır. Ayrıca mevcut sağlayıcıların hizmetlerinden yararlanan müşterilerin, sağlayıcı değişikliği sürecinde yaşayabileceği ciddi sorunlar; mevcut bulut müşterilerinin yeni sağlayıcılara yönelmesini daha da zorlaştırmaktadır. Bu sebeple bu kuruluşlar için piyasada kendine yer açıp, müşteri kazanmak, ancak yeni veya farklılaşmış ürün ve hizmetler sunarak mümkün olabilecektir. Bu durum bulut bilişim pazarının gelişimi açısından önemli bir tehdittir.

Bulut bilişim açısından diğer bir tehdit ilgili standart ve mevzuatlar konusunda yaşanan yetersizlik ve belirsizliklerdir. Bulut mimarileri sürekli yeni iş modelleri geliştirilen ve ilerleyen sistemler olmalarına rağmen, yasa ve standartlar bu hızlı değişime ve gelişime ayak uyduramamaktadır. Yaşanan belirsizlikler geliştirilen

teknolojilerin kısa vadede katma değer elde etmesini engeller. İlgili yasal çerçevenin çizilmesi, bulut bilişimle ilgili şeffaflık ve güvenilirliği artıracak ve yaşanan birçok sorunu engelleyecektir.

Kendi özel bulut altyapılarına sahip olanlar hariç, bulut kullanıcıları güvenlik konusunda sağlayıcıya ve/veya onun sunduğu hizmeti veya bir bölümünü taşere ettiği bir üçüncü kuruluşa güvenmek zorundadırlar. Güvenlik problemleri, güvenilirlik sorunu yaratarak, bulut bilişimin ana zayıflıklarından birini oluşturur. Veri ve uygulama güvenliğinin temelde sağlayıcının sorumluluğunda olduğu düşünülse de, birçok durumda hizmeti kullanan müşterinin de dikkatli ve özenli davranması şarttır. Özellikle veri mahremiyetinin ön planda olduğu uygulamaları sunan büyük ölçekli müşterilerin, güvenlik açıklarına toleranslarının az olması, bulut teknolojilerine geçişte tereddütler yaşamalarına sebep olabilecektir. Bu sebeple sağlayıcıların, bilgi güvenliği seviyesi yüksek iş modelleri oluşturarak, müşteri hedef kitlelerine hizmetlerinin güvenlik zafiyeti yaşamayacağını taahhüt edebilmeleri gerekecektir. Bunu yapamayan zayıf sağlayıcılar zamanla pazarı terk etmek zorunda kalacaktır.

Bulut bilişim ile ortaya çıkan diğer bir tehdit, bulut bilişime geçiş yapmaya hazırlanan birçok şirketin, bu teknoloji sayesinde kendi mevcut bilişim personelinin yürüttüğü birçok bilişim hizmetini dış kaynak kullanım yoluyla sağlaması sonucu, ilgili personelin atıl duruma düşerek işlerini kaybetmeleri olasılığıdır. İleri derecede yönetim sistem ve otomasyonlarını standart olarak sağlayan bulut altyapılarının, küresel ölçekte bilişim personeli ihtiyacını düşüreceği açıktır. Bu durum, bu personelin istihdamına yönelik önemli bir tehdit unsurudur.

E-keşif yoluyla mahkemelerin kullanıcılara ait verileri talep etmesi durumu, bulut bilişim mimarileri için diğer bir tehdittir. Bulut müşterileri, sağlayıcıdan edindikleri hizmete bağlı olarak çoğunlukla verilerinin depolandığı yeri bilmezler ve bilseler dahi, bu veriyi mahkemece talep edilen formatta ve kısa sürede temin etmeleri zor olabilir. Ayrıca ilgili davada müşterinin yanında bulut sağlayıcının da taraf olması, müşterinin verisi üzerindeki kontrolünü kaybetmesine sebep olabilir. Bu sebeple

sağlayıcılar ile yapılan hizmet seviye anlaşmalarında, bir mahkemenin veri talebi durumunda, veri kontrolünün ne şekilde sağlanacağı açıkça belirtilmelidir.

BULUT BİLİŞİM SWOT ANALİZİ TABLOSU			
Güçlü Yönler	**Fırsatlar**	**Zayıf Yönler**	**Tehditler**
Düşük Maliyet Uzman Personel İhtiyacının Azalması Esneklik ve Ölçeklendirilebilirlik Verimlilik Lokasyon Bağımsız Erişim	Yenilikçi Teknoloji Yeşil BT Karmaşıklık Yeni Pazar Olanakları	Kontrol Kaybı Sağlayıcıya Bağımlılık Güvenilirlik Küresel Ekonomiye Duyarlılık	Piyasa Rekabeti Standart ve Mevzuat Yetersizliği Güvenlik Atıl Bilişim Peroneli E-Keşif

Tablo.1.1: Bulut Bilişim SWOT Analizi

2. BULUT BİLİŞİM İLE KAMU HİZMETLERİNİN ENTEGRASYONU

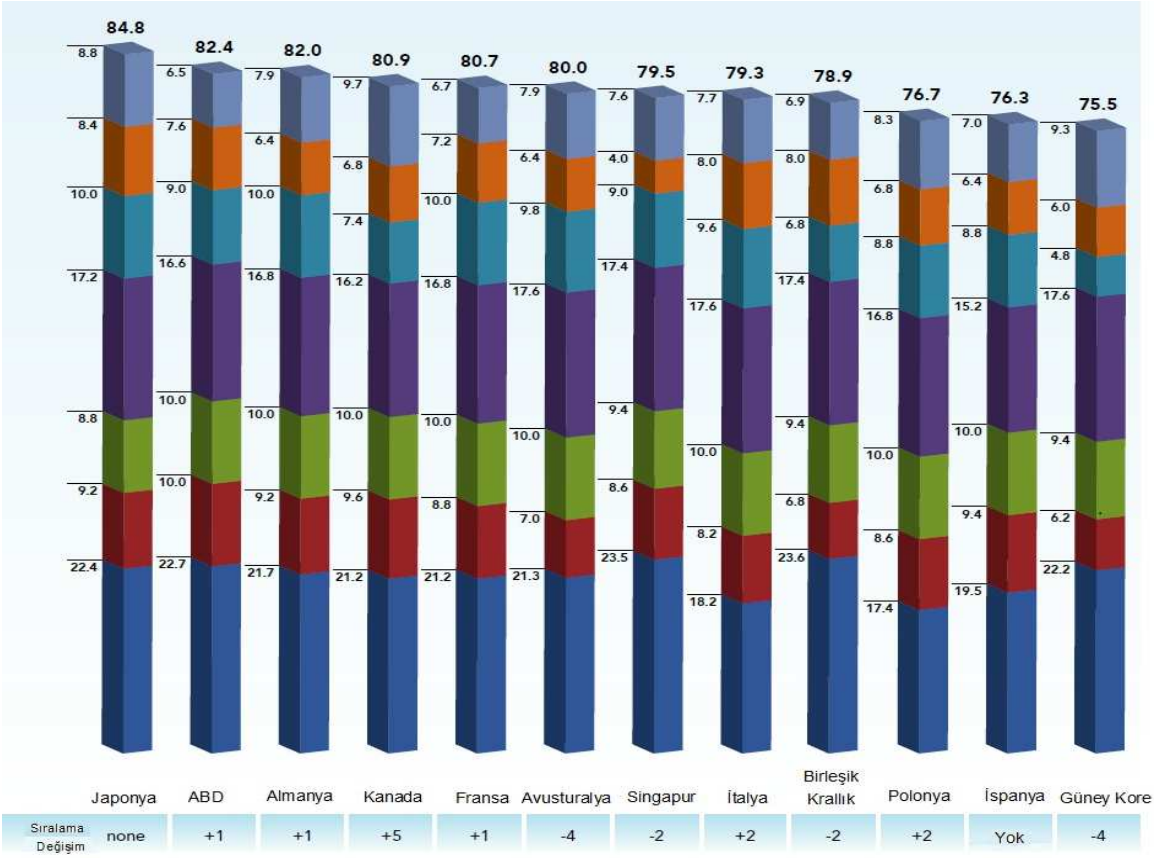
Bulut bilişimin bilgi teknolojilerine getirdiği yenilik ve avantajlar, kısa zamanda özel sektör kuruluşları gibi kamu kurum ve kuruluşlarının da ilgisini çekmiştir. Geçmişte vatandaşların yararlanması amacıyla, çok sayıda personel tarafından devlet dairelerinde verilen kamu hizmetlerinin önemli bir bölümünün internet ortamında sunulabileceğinin görülmesi, kuruluşları ilgili hizmetlerin sunumuna yönelik web arayüzleri ve uygulamalar geliştirmeye yöneltmiştir. Farklı uygulamaların, farklı alan adları altında sunumu ve bu durumun yarattığı karmaşıklık, kamu hizmet arayüz ve uygulamalarına tek bir platformdan erişebilme gereksinimini ortaya çıkarmış ve bu da e-devlet platformlarının geliştirilmesini sağlamıştır. Kamu kurum ve kuruluşları, e-devlet platformlarına servis ettikleri uygulamaların barındırılması ve işletilmesi için daha gelişmiş veri merkezleri kurma ve işletme arayışına girmiş ve bu durum kuruluşların bilişim altyapı ve işletme maliyetlerini artırmıştır. Maliyetlerde yaşanan bu artış ve nitelikli bilişim uzmanı istihdamında yaşanan zorluklar, devletleri farklı kuruluşların bilişim hizmetlerinin hepsini veya bir kısmını entegre veri merkezleri üzerinden sunmaya yöneltmiştir. Bu doğrultuda, Güney Kore 48 adet merkezi kamu idaresinin bilgi sistemlerini 2 ayrı şehre konumlandırılacak şekilde tek bir veri merkezinde birleştirmiş, Amerika Birleşik Devletleri ise bulut bilişim ve ortak veri merkezi yaklaşımlarıyla kısa vadede 800 adet veri merkezini kapatarak, veri merkezi sayısını yüzde 40 oranında azaltmayı planlamıştır.

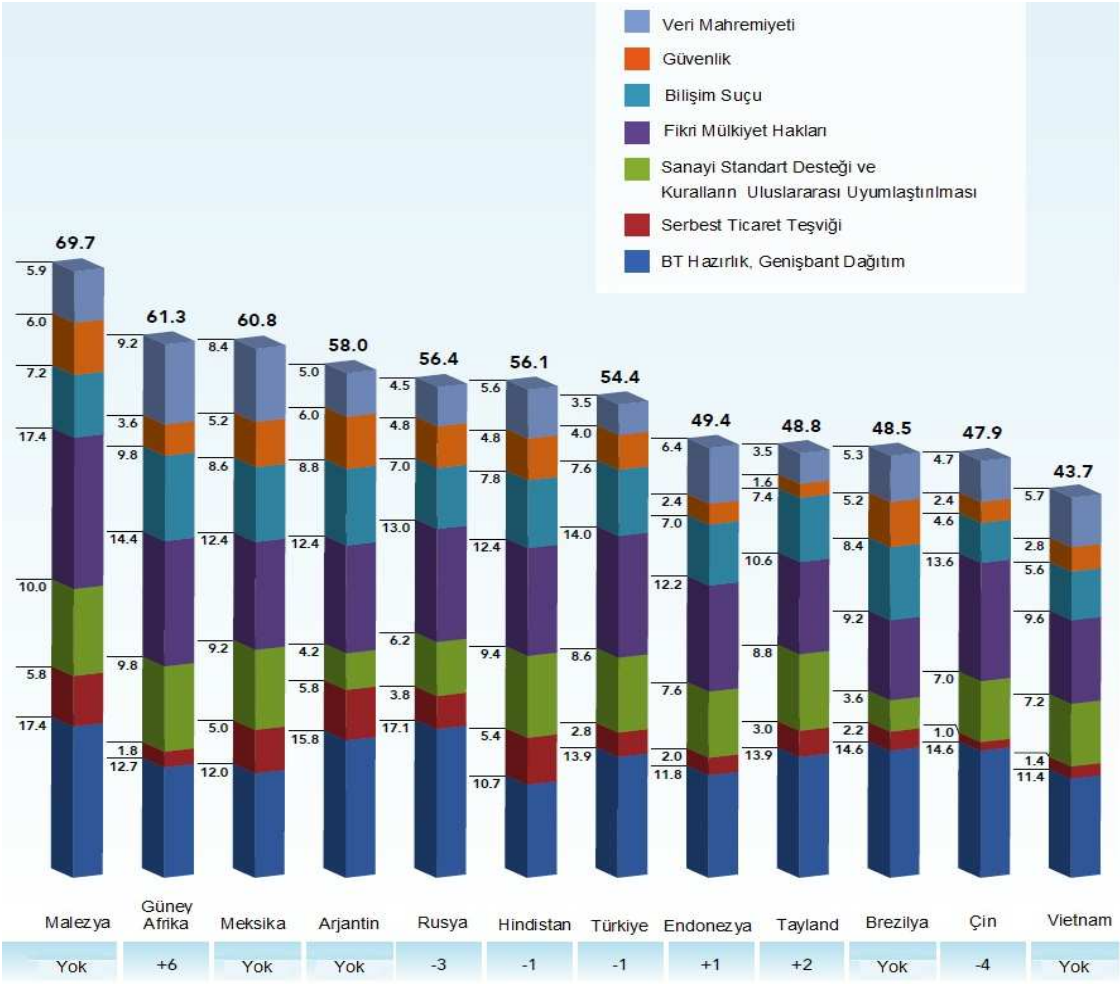
Ülkemizde de idari ihtiyaçlar, tasarruf imkânı ve siber güvenlik gereksinimleri doğrultusunda, halen her kurumda müstakil olarak işletilmekte olan veri merkezlerinin tek bir çatı altında birleştirilerek Türkiye Kamu Entegre Veri Merkezi'nin kurulması önem arz etmektedir. Bu doğrultuda, Bilim ve Teknoloji Yüksek Kurulu (BTYK) 25. Toplantısında alınan 2013/104 sayılı karar uyarınca, kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir. Bu sayede yedeklilik, felaket kurtarma merkezi, siber

güvenlik, iş sürekliliği, kamu bulutu, işletme maliyeti, kurumlar arası veri paylaşımı gibi hususların tamamına çözüm sağlanması amaçlanmaktadır.

2.1. Bulut Bilişim İle İlgili Dünya Örnekleri

BSA The Software Alliance adlı kuruluş tarafından yayımlanan 2016 BSA Global Bulut Bilişim Puan Çizelgesi adlı araştırma, dünya BT pazarının yüzde 80'ini oluşturan 24 ülkeyi, bulut bilişime ne oranda hazır olduklarıyla ilgili değerlendirmekte ve sıralamaktadır. Her ülke, yedi kilit politika alanında güçlü ve zayıf yönleri üzerinden değerlendirilmektedir. Bunlar veri mahremiyeti, güvenlik, bilişim suçları, fikri mülkiyet hakları, sanayi standart desteği ve kuralların uluslararası uyumlaştırılması, serbest ticaret teşviği ve BT hazırlık ve genişbant dağıtımı olarak sıralanmaktadır. Aşağıda ilgili 24 ülkenin, anılan yedi kilit politikaya göre sıralandığı tablo bulunmaktadır (BSA, 2016).





Tablo 2.1: 2016 BSA Global Bulut Bilişim Puan Çizelgesi (Kaynak: BSA, 2016)

Amerika Birleşik Devletleri

2016 yılı BSA Puan Çizelgesinde ikinci sırada yer alan Amerika Birleşik Devletleri gerek e-devlet uygulamaları ve gerekse de bulut bilişim teknolojisi ve bu teknolojinin gelişmesine ön ayak olan öncül teknoloji ve yeniliklerin birçoğunun ilk olarak ortaya çıktığı, kullanıldığı ve dünyaya yayıldığı ülke konumunda bulunmaktadır. Bu bölümde öncelikle ABD'nin bulut bilişimin kullanımı ve yaygınlaştırılması ile ilgili

politika ve stratejilerine, sonrasında ise kamu kuruluşları tarafından kullanılan önemli bulut bilişim hizmet platformlarına yer verilecektir.

ABD'nin bulut bilişim konusunda uygulamaya koyduğu ilk stratejilerden biri Önce Bulut Politikası'dır. Bu politika kamu kuruluşlarında özel bulutların oluşturulması ile ilgili strateji ve hedefleri ortaya koymaktadır. Bu politika, Beyaz Saray Yönetim ve Bütçe Dairesi tarafından 2010 yılının Aralık ayında hazırlanan ve ülke çapında BT yönetiminde reform yapmaya yönelik olan; "Federal Bilgi Teknolojileri Reformu için 25 Maddelik Uygulama Planı" nın bir parçasıdır. Burada, temel amaç kamuda daha düşük maliyetli teknolojilerin ve ortak hizmetlerin kullanımını teşvik ederek, işlevsel verimliliği arttırmaktır. Politikaya göre, her kamu kurumunun, politikanın yayımlanmasını müteakip 3 ay içinde bulut bilişime taşınması gereken 3 sistemini belirlemesi, 12 ay içinde bunlardan birini ve 18 ay içerisinde de kalan ikisini bulut ortamına taşıması gerekmektedir (Kundra, 2010). Bu politika, kamuda bulut bilişime geçişin hızlandırılması amacıyla kamu kuruluşlarını, bilişim hizmeti temininde düşük maliyetli ve güvenilir bulut bilişim çözümlerine öncelik vermeye ve tercih etmeye zorlamaktadır.

Önce Bulut Politikası ile ortaya konan bulut bilişim stratejisinin hayata geçirilmesi amacı doğrultusunda, ABD Bilişim Kurulu tarafından 2011 yılının Şubat ayında yayımlanan Federal Bulut Bilişim Stratejisi; kamu kurumlarının veri merkezlerinde gözlenen; kaynak kapasite kullanım oranlarının düşüklüğü, tedarik sürelerinin uzunluğu, kaynak yönetiminin güçlüğü, talep yapısının parçalı oluşu, gereksiz tekrarlanan sistemlerin bulunması gibi sorunların, kamu hizmetlerini olumsuz yönde etkilediği ve bulut bilişimin söz konusu sorunların giderilerek kamu hizmetlerinin iyileştirilmesinde etkili olabilecek potansiyele sahip olduğu düşüncesinden hareketle hazırlanmıştır. Buna göre, söz konusu stratejinin amacı,

- Bulut bilişimin getirilerini, güçlüklerini ve bunların dengesini ortaya koymak,
- Kamu kurumlarının bulut bilişime geçişine yardımcı olacak bir karar modeli ve çeşitli uygulama örnekleri sunmak,

- Bulut bilişim uygulama kaynaklarını vurgulamak,
- Bulut bilişimin benimsenmesini kolaylaştırma hususunda yürütülen çalışmaları belirtmek ve kurum ve kuruluşlara düşen rol ve sorumlulukları belirlemektir.

Federal Bulut Bilişim Stratejisinin yayımlanmasını müteakiben, her kamu kurumunun kendi BT tedarik stratejisini gözden geçirerek, kaynak tedariğinde bulut bilişim hizmet modelini de bir alternatif olarak ele alacak şekilde güncellemesi beklenmektedir (Türkiye Bilişim Derneği, 2012).

Federal Bulut Bilişim İnsiyatifi, kurumlarda ortak olarak kullanılan hizmetlerin ve çözümlerin tespit edilmesi ve bulut bilişim modelinin kullanılması suretiyle, BT hizmetlerinin modernize edilmesini amaçlayan ve Başkanlık düzeyinde kabul gören bir insiyatiftir. ABD Yönetim ve Bütçe Dairesi ile Federal Bilişim Kurulu tarafından başlatılan bu insiyatifte bulut bilişim kilit bir rol üstlenmektedir.

Federal Bulut Bilişim İnsiyatifinde görev alan kuruluşlardan biri olan ABD Genel Hizmetler Dairesi (GSA), kamu hizmetlerinde işlevsel verimliliğin arttırılması, ortak hizmet ve çözümlerin kurumlar arasında paylaşılması ve şeffaflığın, işbirliğinin ve katılımcılığın sağlanmasına katkıda bulunacak bulut bilişim çözümlerinin tedarik edilmesi ve kullanılmasına yönelik projeler yürütmektedir (Türkiye Bilişim Derneği, 2012).

GSA'nın diğer bir görevi, federal hükümetin e-devlet portalları olan ve yılda 140 milyondan fazla vatandaşın ziyaret ettiği, bulut tabanlı USA.gov ve İspanyolca dilindeki benzeri GobiernoUSA.gov'u sunmaktır. GSA, hizmetleri için geliştirilmiş ve ölçeklenebilir web servislerini sunarak, kuruluşun idari masraflarını yarıya yarıya ve altyapı maliyetlerini de yüzde 90 oranında düşürmeyi başarmıştır (Mahmood, 2015).

GSA, güvenlik, gizlilik ve operasyonel yetenekleri açısından sertifikalandırılmış, ön yeterliliğe sahip satıcılar aracılığıyla tüm federal kurumlar için, talepleri doğrultusunda Servis olarak Altyapı (IaaS) temin etmeyi ilke edinmiştir. GSA ayrıca, kamu kuruluşlarının bulut tabanlı hizmetler temin etmelerini kolaylaştırmak ve ilgili

hizmet ihtiyaçları için kendi bünyelerinde veri merkezleri oluşturmalarını engellemek amaçlarıyla, hem kendi ve hem de özel sektör tarafından geliştirilmiş en işlevsel kamu uygulamalarını tanıtan ve bu uygulamaları satın alma şartlarını belirten bir bulut bilişim mağazası olan Apps.gov kurmuştur. Bu platform üzerinden kamu kuruluşları, ilgili hizmet sağlayıcısının ihtiyaç duydukları ürününü temin edebilmekte ve ihale şartları konusunda yardım alabilmektedir (Mahmood, 2015).

Birleşik Krallık

2016 yılı BSA Puan Çizelgesinde dokuzuncu sırada yer alan İngiltere bir kamu bulutu örneği olan bulut bilişim ağı G-Cloud'u geliştirmiştir. G-Cloud bünyesinde, kamu kuruluşlarının satın almak istedikleri hizmetler için arama yapabilecekleri bir online mağaza olan "Dijital Pazaryeri" ve ihale sürecine ihtiyaç duymadan hizmet satın alabilmeleri için bulut tedarikçisi firmalarla yapılmış bir dizi çerçeve anlaşma bulunmaktadır. Dijital Britanya stratejisi, geleceğin BT ekonomisine öncülük etmeyi ve kamu kuruluşlarına bu konuda araçlar temin etmeyi amaç edinmiştir. Dijital Britanya stratejisinin önemli bir yönü, kamunun bilgi teknolojisi altyapısının geliştirilmesi amacıyla; büyük çapta hizmetin çevrimiçi sunulmasına izin vermesi olmuştur.

İngiltere'de bulut teknolojileri, merkezi hükümetin maliyetlerini düşürmeye ve küçük ve orta ölçekli işletmelerin (KOBİ), kamu sektörüne daha fazla hizmet satmasına yardımcı olur. Kamu Dijital Hizmetleri olarak adlandırılan temel BT grubu, kamu kuruluşlarını, kendi bilgi teknolojilerini bulut bilişime dönüştürmek için teşvik etmektedir. Bu grup Birleşik Krallık Kabine Ofisi'ne bağlıdır ve kamu kuruluşlarını maliyetlerini düşürmek ve veri merkezlerini rasyonalize etmek konularında cesaretlendirmektedir. Ayrıca iç ve dış sağlayıcılar arasındaki rekabeti tesis ederek, maliyetleri düşürmek için de çalışmaktadır (Gov.Uk., 2013).

İngiltere ayrıca 2013 yılında G-Cloud sağlayıcı çerçevesini genişleterek, Amerika Birleşik Devletleri benzeri bir "önce bulut" politikası ortaya koymuştur. Bu politika kamu sektöründe BT satın almak isteyen her kuruluşun, öncelikle bulut teknolojileriyle ilgili araştırma yapması gerektiği ile ilgilidir. İngiliz hükümetini

denetleyen Ulusal Denetim Ofisi, hükümetin BT reformlarını ve ilgili tasarruf tedbirlerini sürekli denetlemekte ve ayrıca daha çevik ve daha verimli olup olamayacağını görmek için kamu kuruluşlarının BT'lerini nasıl idare ettiğini incelemektedir.

Altyapı bağlamında İngiltere, 2017 yılına kadar ülke genelinde süper hızlı internete geçerek, indirme hızlarını en az 2 Mbps'e çıkarmayı, ayrıca ev ve işyerlerinin % 95'ine 24 Mbps hızda internet sağlamayı hedeflemektedir (BSA, 2016).

Japonya

Japonya Business Software Alliance (BSA) Küresel Bulut Bilişim Puan Tablosunda (2016) ilk sıradadır. Özellikle gizlilik politikaları ve siber suçların önlenmesi ile ilgili ciddi ilerleme kaydeden ülke, bu tabloda puanını daha da artırarak yerini korumuştur. Tablo 2.1'de yer alan bu Puan Kartında bulut bilişimle ilgili farklı renklerle işaretlenmiş farklı faktörler göz önünde bulundurularak, ülkeler her bir faktör için ayrı ayrı puanlanmış ve hesaplanan toplam puana göre ülkelerin bulut bilişim gelişmişlik sıralaması yapılmıştır. Japonya'nın bulut bilişim alanında başarılı olmasında, politika yapıcıların ülkenin Japon teknolojisi haricindeki dış teknolojilere kolay adapte olamadığını göz önünde bulundurarak tebirler almalarının etkisi büyük olmuştur. Batı menşeli bir teknoloji olan bulut bilişimin, müşteri haklarına riayet edecek şekilde geliştirilmesi ve sunulması konusunda politikacıların ciddi çalışmaları mevcuttur. Ancak ağ, donanım, uygulamalar ve platformlar gibi çeşitli sektörleri tek çatı altında toplayan bulut bilişim mimarisinin yaratacağı sorunlarla ilgili tekil politikalar yeterli olamayacağından, oluşturulan politikaların farklı alanlara uyarlanabilecek esneklikte olmasına dikkat edilmektedir. Yine Japonya İçişleri ve İletişim Bakanlığı (MIC) tarafından Nisan 2009'da Dijital Japonya Dönüşüm Projesi başlatılmıştır (MIC, 2009).

Kasumigaseki Bulutu, tüm devletin BT ihtiyacını, tek bir bulut altyapısı altında konsolide olarak ele alan büyük bir bulut bilişim girişimi olup, birçok bakanlığının bulunduğu Tokyo'nun ilgili bölgesinin ismini almıştır (Hicks, 2009). Bu girişimle, Japon hükümetinin tüm bilgi işlemine ev sahipliği yapacak bir özel bulut ortamı

geliştirilmiştir. Japonya Kasumigaseki bulutuyla; daha fazla bilgi ve kaynak paylaşımını sağlamak, devletin BT kaynaklarında daha fazla standardizasyon ve konsolidasyon sağlanmasına katkıda bulunmak, maliyetleri azaltmak, işletme faydaları ve daha çevre dostu BT operasyonları sağlamayı hedeflemektedir. Kasumigaseki Bulutu, Dijital Japonya Dönüşüm Projesinin bir parçası olup, BT yatırımlarını kullanarak (hemen hemen 100 trilyon yen değerinde) ekonomik canlanmayı teşviğe yardımcı olmak için; önümüzdeki birkaç yıl içinde birkaç yüzbin yeni BT iş olanağı yaratılması ve 2020 yılına kadar Japonya'nın BT pazarının büyüklüğünün iki katına çıkarılmasını amaçlayan bir devlet girişimidir (MIC, 2009).

Japonya, bulut teknolojisi ile yakın zamanda tanışmış olsa da; yerel telekom şirketleri, iç pazarda hızla artan talepleri karşılamak amacıyla ve aynı zamanda kendi hizmetlerinin küresel olarak tercih edilmesi umuduyla agresif bir şekilde bulut bilişim altyapıları inşa etmeye devam etmektedirler. Bu doğrultuda, birçok Japon KOBİ'si bulutu benimsemeyi düşünmektedir. KOBİ'ler için bulut hizmetlerinin kullanılması, işgücü verimliliğinin artırılmasını ve gereksiz maliyetlerin azaltılması sağlayabilecektir. Ayrıca bulutun ölçeklendirilebilir yapısı, KOBİ'lerin planlı bir şekilde büyüyebilmesine olanak sağlar.

Avrupa Birliği

2012 yılı sonbaharında Avrupa Komisyonu, Avrupa Birliği içinde bulut bilişimin benimsenmesini teşvik etmek ve Avrupa tek pazarı içinde bulut teknolojilerinin kullanımının artması için ilk adım olarak, Avrupa Birliği Bulut Bilişim Stratejisini başlatmıştır. Avrupa Komisyonu, ortaya çıkan BT pazar büyümesinin, Avrupa bulut bilişim kullanıcıları ve sağlayıcılarının her ikisinin de yararına olacağına belirterek, yasama organlarını etkili küresel bir yaklaşım geliştirmek için teşvik etmiştir.

30 Avrupa ülkesinde bulunan ve kar amacı gütmeyen bağımsız Avrupa kuruluşlarından oluşan, EuroCloud Avrupa adında bir federasyon kurulmuştur. EuroCloud'un genel misyonu ve amacı; Avrupa'da bulut bilişim pazarını teşvik etmek

ve faydaları hakkında kamuoyunu bilinçlendirmektir. Organize edilen yıllık etkinlikler sayesinde EuroCloud, Avrupa endüstrisiyle bilgi paylaşımını kolaylaştırmayı, kontak ağı oluşturmayı ve stratejik ittifaklar kurulmasına ön ayak olmayı hedeflemektedir. Avrupa Komisyonu, EuroCloud'un Brüksel'deki ofisi aracılığıyla, bulut endüstrisinin standardizasyonu çalışma gruplarına (güvenilirlik, belgelendirme ve birlikte çalışabilirlik) katılım sağlamaktadır. İki yıl içinde EuroCloud, Romanya da dâhil olmak üzere 18 ülkede kurulan temsilcilikleriyle, 27 Avrupa ülkesinde faaliyet gösterir hale gelmiştir. Bu ülkelerdeki temsilciliklerin yönetim kurullarının üyeleri, EuroCloud Avrupa'nın da üyeleridir ve Avrupa düzeyinde alınacak olan her kararda birer oy sahibidirler (Iovan, 2013).

Almanya

Almanya 2016 BSA sıralamasında üçüncü sırada olup Avrupa Birliği ülkeleri arasında ilk sıradadır. Bu sıralamaya rağmen Almanya, vatandaşların veri gizliliği ve güvenliği ile ilgili endişe duymaları sebebiyle, bulut hizmetlerini benimseme konusunda bir miktar geri kalmıştır. Örneğin Almanya hükümeti, beş büyük bilişim tedarikçisiyle, temin ettiği hizmetleri İngiltere'nin G-Cloud kamu bulutuna benzer şekilde konsolide etmek için sözleşme müzakereleri yapmış fakat bir sonuca varamamıştır. Ayrıca web barındırma hizmeti ve erişim sağlayıcılarının, kendi sistemlerinde meydana gelen telif hakkı ihlallerinden, Medeni Kanun çerçevesinde sorumlu olup olmadıkları hakkında devam eden bazı belirsizlikler bulunmaktadır (Mahmood, 2015).

Ancak bütün bu olumsuzluklara rağmen Almanya yasal olarak sağlam bir altyapıya sahip olduğundan, 2016 BSA sıralamasında ilgili sıralamayı edinebilmiştir. Örneğin Almanya'da kapsamlı bir siber suç mevzuatı ve güncel bir fikri mülkiyet koruması mevcuttur. Almanya'da aynı zamanda modern elektronik ticaret ve elektronik imza yasaları vardır. Bu yasaların kombinasyonu, Almanya'da bulut bilişim hizmetlerinin gelişebilmesi için temel teşkil etmektedir. Almanya'nın, uluslararası standartlar ve birlikte çalışabilirlik için güçlü bir taahhüdü ve nüfusun genişbant

erişiminin artırılması ile ilgili iyi bir ilerlemesi vardır. 2018 yılına kadar ev tipi kullanıcılara en az 50 Mbps hızında internet sağlanması hedeflenmeketedir (BSA, 2016).

Federal düzeyde, bazı pilot bulut aktarım örnekleri olsa da, eyaletlerin ve şehirlerin bulut bilişim mimarilerini benimsemeleri daha kolay olmaktadır. Buna iyi bir örnek, Berlin'in sakinlerine kamusal ve ticari hizmetler için güvenli erişim sunan ve bulut tabanlı bir pazar olan goBerlin'dir. Proje, kamu BT hizmet sağlayıcısı ITDZ Berlin'in mevcut bulut altyapısı üzerine inşa edilmiştir. Küçük ve orta ölçekli işletmeler ve yerel yönetimler için Servis olarak Yazılım (SaaS) sağlayarak, bu kuruluşların IT hizmetlerini geliştirme ve kullanmaları konusunda önemli bir rol oynamaktadır. Berlin metropolü sınırlarında yapılan pilot bir uygulamada, sakinler bir e-kimlik kartı kullanarak entegre bulut hizmetlerini en iyi şekilde elde etmişlerdir. Projenin temel amacı; gelişmesi ve büyümesi için goBerlin'i teşvik edecek, güçlü kullanıcı ve geliştirici toplulukları oluşturmaktır (Fokus, 2013).

Fransa

2016 BSA sıralamasında beşinci sırada yer alan Fransa da, kamuda bulut bilişim teknolojilerini benimsemek konusunda yavaş kalmıştır. Bu durum, devam eden bilişim yatırım ve harcamalarının aniden kesilmesinin, sosyal etkiler yaratacağı düşüncesinden kaynaklanmaktadır. Fransa hükümeti, kendi sınırları içinde barındırılan tüm veri ve hizmetleri işletmeyi vaat etmiş ancak sadece kendi iç dönüşümünü esas alan bir hamleyle yetinmiştir. Devlet stratejisinin iki bileşeni vardır. Bunların birincisi, başbakanın merkezi yönetim organlarından biri olan Hukuki ve İdari Bilgiler Müdürlüğü'nün (DILA), özel bir bulut oluşturmak için görevlendirilmesidir. Bu özel bulut, DILA ve diğer devlet bakanlıkları tarafından kullanılacak şekilde tasarlanacaktır. İkincisi ise, büyük GSM operatörleri tarafından yönetilen ve işletilen iki özel sektör "egemen bulutu" oluşturulmasına sponsor olmasıdır. Bu sponsorlukla, Fransa içindeki kamu ve özel sektör kuruluşları tarafından kullanılabilecek, halka açık, çok kiracılı bulut hizmetleri sağlanması hedeflenmiştir. Sponsor olunan bu iki bulut, Orange şirketi tarafından yönetilen CloudWatt ve SFR şirketi tarafından işletilen Numergy'dir

(Accenture, 2013). Bu bulutlar hali hazırda kamu ve özel sektör kuruluşları tarafından kullanılmaktadır.

Fransa kamu kuruluşları için ülke çapında kamu bulutu kurulumunu ve gelişimini tercih etmiştir. 2011 yılında "Andromeda" adlı kendi kamu bulutunu geliştirmeye başlamıştır. Bu kamu bulutu, kamu kuruluşları için bir SaaS platformu kurmak için Orange ve Thales şirketleri tarafından hayata geçirilmiştir. Bu özel kamu bulutunun geliştirilmesinin temel amacı, veri koruma ve güvenlik açısından ulusal yasalara tam uyumu garanti edebilecek şekilde tasarlanabilmesidir. Aksi takdirde, başka bir ülke, örneğin ABD merkezli hizmetleri benimseyerek oluşturulacak hizmet modellerinin, ulusal mevzuata uyumlu olması çok zor olacaktı (Mahmood, 2015).

Yerel bazda Paris belediyesi, bulut tabanlı bir intranet oluşturmak için özel sektör kuruluşlarıyla güçlerini birleştirmiş ve orta dereceli okulların ders materyallerini ve diğer bilgileri paylaşmak için bulut platformu kullanmaya başlamıştır.

İspanya

İspanya'da kamu sektöründe bulut bilişimin benimsenmesi hala çok sınırlıdır. Bunun nedenleri, kamu kuruluşlarının veri bütünlüğü, gizliliği ve yasalar ile ilgili endişeleri olarak sıralanabilir. Merkezi hükümet, bulut teknolojilerinin benimsenmesini yeterli düzeyde teşvik etmemekte olup, yerel yönetimlerin belli bir çabası mevcuttur. Yerel yönetimler, merkezi yönetimin aksine sınırlı bir mali kapasiteye sahiptirler ve bu sebeple bulut bilişimin sağlayacağı maliyet tasarruflarına ihtiyaç duyarlar. Bu sebeple birçok yerel yönetim kuruluşu bulut bilişimi benimsemiştir. İspanya'da en çok tercih edilen bulut mimarisi özel bulut (yaklaşık % 58) olup, bunu açık bulut (yaklaşık % 31) ve hibrit bulut (yaklaşık % 17) takip etmektedir. Özel bulut, güvenlik ve gizlilik açısından yüksek kontrol sağlaması nedeniyle tercih edilmektedir. Topluluk bulut mimarisi ise sadece belirli sektör uygulamalarını (örneğin sağlık) hedef seçetiği için, İspanya'da nadiren kullanılmaktadır (Zwattendorfer, 2013a).

15 Ocak 2013 tarihinde, E-Devlet Yüksek Kurulu İspanya'da kamuya yönelik özel bir bulut oluşturmak için öncelikli proje olarak Sara'yı belirlemiştir. Sara, kamunun mevcut altyapısı üzerinde bulut bilişimin ilk adımlarını atmıştır. Sara, merkezi yönetimin yanı sıra, bölgesel ve yerel yönetimlere de entegre edilmiş ve hizmet sağlamaya başlamıştır. Hâlihazırda, kamuda e-sertifika doğrulaması için @firma platformu ve veri haritalama platformu gibi yaygın paylaşılan hizmetleri sunmaktadır. Yine Katalonya hükümeti, daha etkin bir bilişim hizmeti temin etmek amacıyla, devletin veri merkezlerini bulut tabanlı altyapıya dönüştürmek için, HP firması ile 67.000.000 $ tutarında bir sözleşme imzalamış olup, bu sözleşme 10 yıl boyunca geçerli olacaktır. (Government of Spain, Ministry of Finance and Public Administration, 2013).

Çin

2016 BSA sıralamasında yirmi dört ülke arasında yirmi üçüncü sırada yer alan Çin'de, bulut bilişim devletin güçlü desteğiyle hızla büyümektedir. Çin Yazılım Endüstrisi Birliği'ne göre ülkenin toplam bulut bilişim değeri 2015 yılına kadar en az 122 milyar dolar olacaktır. Ülke küresel bulut bilişim pazar payının henüz % 3'ten daha azını teşkil etmesine rağmen, yıllık % 40'lık oran ile hızla büyümektedir (Jones, 2012).

Çin'in bulut bilişim piyasasında genişlemesi, 2011 yılında hükümetin 12. Beş Yıllık Planında bir öncelik olarak ilan edilmiştir. 2013 yılında, Çin'de devam en az 40 açık bulut projesi olup, sadece Pekin şehrinin veri merkezi inşa etmek ve diğer altyapıları desteklemek için devletten aldığı kaynak 8 milyar doların üzerindedir. Kolay veri depolama ve düşük bakım maliyetleri Çin'de bulut bilişim benimsenmesini tetikleyen en önemli faktörlerdir. Çin, dünyanın en büyük internet kullanıcısı nüfusuna sahip olup, 2013 yılı sonuna kadar ülkede, bulut tabanlı yazılım ve uygulamalara erişilebilen 500 milyon akıllı telefon bulunacağı beklenmektedir (Larson, 2013).

Ulusal Bulut Bilişim Sanayi'nin başlattığı 'Çin Bulutu' kalkınma planı, 2012 yılında Devlet Konseyi tarafından onaylanmıştır. Bu plan, 12. Beş Yıllık Dönemde Çin'in bulut bilişim sektörü için; kalkınma stratejisi, teknoloji yol haritası, destek

sistemleri gibi bulut stratejilerinin geniş bir yelpazesini kapsamaktadır. Ayrıca, Sanayi ve Bilgi Teknolojileri Bakanlığı, diğer ulusal birimlerle birlikte, 2010 yılının ikinci yarısında pilot ve demonstrasyon projeleri aracılığıyla yenilikçi bulut bilişim hizmetlerinin geliştirilmesine ilişkin talimatlarını açıklamıştır. Buna göre Pekin, Şangay, Shenzhen, Guangzhou ve Wuxi şehirleri bulut bilişim hizmetlerinin geliştirilmesi için öncü bölgeler olarak sıralanmıştır. Çin ayrıca bulut bilişim tanıtım projeleri için, bu öncü beş şehirde uygulanacak 12 anahtar teslim projeye, toplam 1.5 milyar Yuan yatırım bütçesi tahsis edilmesini sağlayan Ulusal Mali Destek Programı onaylamıştır.

Çin'de bulut bilişim teknolojisinin ilk büyük ölçekli kullanımının kamu tarafından gerçekleştirilmesi beklenmekteydi. İşyerinde verimlilik artırmaya yardımcı olan ve vatandaşlara daha iyi hizmet veren bulut bilişim tabanlı e-devlet sistemleri, kamu sektörü için kolaylaştırıcı olarak görülmekteydi. Bu sebeple Çin hükümeti, e-devlet gelişimi için bu yönde bir strateji belirlemiş ve pek çok anahtar teslim proje kamu sektörü tarafından başlatılmıştır. 2011 yılının Mart ayında, Çin'in için ilk sağlık bulutu olan Shanghai Shibei Hastanesi Sağlık Bulut Sistemi kullanıma girmiştir. Ayrıca, 2011 yılı Temmuz ayında, Xi'an şehrinin Yüksek Teknoloji Bölgesi, Dual Bulut Dağıtım Stratejisi ilan etmiş ve Kuzeybatı Çin'deki ilk bulut bilişim veri merkezi olan Xi'an Yazılım Parkı'nı, işletmeler ve şirketlere Servis olarak Altyapı (IaaS) sağlamak için inşa etmiştir. Çin'in kamu sektörü BT yatırımlarının 2011 yılında 46.4 milyar Yuan'dan, 2012 yılında 50.29 milyar Yuan'a büyümesi beklenmektedir (Jones, 2012).

Diğer Ülkeler

Avrupa'da, Avusturya'nın bulut bilişim mimarisini benimsemesinin temel nedeni maliyet tasarrufudur. Ama maliyet tasarrufu avantajına rağmen bulut mimarileri yönetim, güvenlik ve veri koruma gibi sorunları ortaya çıkarmaktadır. Özel ve topluluk bulut mimarilerinin kullanımı yerine açık bulutun kullanılabilmesi için verilerin korunması gibi bazı gereksinimlerin karşılanması gerekmektedir.

Danimarka bilişim maliyetlerini azaltmak için 2009 yılında bir seçenek olarak bulut bilişim teknolojileri ile ilgilenmeye başlamış ve 2011 yılında Danimarka tedarik makamını bir telekom sağlayıcısının bulutu içine taşımıştır.

İrlanda'da hazırlanan bir strateji belgesinde, IBM ve Microsoft'un Dublin'e yakın veri merkezleri işletmesi nedeniyle bulut bilişim, devlet tarafından ekonominin yenilenmesi için önemli bir itici güç olarak tanımlanmıştır (Mahmood, 2015).

Amerika'da, 2009 yılında, Kanada Bayındırlık Hizmetleri Kurumu, Kanada'nın bulut bilişim benimseme stratejisi ile ilgili risklerle faydaları karşılaştıran "Bulut Bilişim ve Kanada Ortamı" başlıklı bir belge yayınlamıştır. 2010 yılında bazı servisler barındıran bir topluluk bulutu sunulmuştur.

Avustralya, 2011 yılında bulut bilişim üzerine bir bildiri yayınlamıştır. Yine bazı kurumlar e-vergi gibi bazı pilot uygulamalar sunmuşlardır. Ülkede c-devlet hizmetleri için servis modeli seçiminde, hizmetlerin düşük risk taşıdığı alanlar için açık bulutlar kullanılmakta, orta riskli hizmetler için topluluk bulutları ve yüksek riskli hizmetlerde özel bulutlar tercih edilmektedir (Mahmood, 2015).

Asya'da, Hindistan bulut bilişimi sınırlı oranda benimsemiştir. Gelecekte benimsenmesi yönünde bir istek olsa da öncelikle güvenlik ve gizlilik gibi sorunların çözülmesi gerekmektedir.

Geçerli portal ve bazı ulusal arşiv veritabanlarının özel bulut unsurlarına dayanmasına rağmen, Malezya'da bulut bilişimin benimsenmesi halen düşük seviyededir. Bulut bilişimin, verimliliğini artırıken, maliyetleri azaltıp, şeffaflığını artırması durumunda ulusal bir girişim olarak tercih edilebileceği ifade edilmektedir (Mahmood, 2015).

Singapur 2011 yılı sonunda özel bulut mimarisine dayalı bulut girişimlerini başlatmış ve bulut bilişimin tüm avantajlarından yararlanmak için bir kamu bulutu oluşturmuştur.

Güney Kore, hem kamu ve hem de özel sektörü desteklemek için bulut tabanlı altyapılara yüz milyonlarca dolar bütçe ayırmıştır. Bu girişim, kamuda BT maliyetlerini azaltırken, küresel pazara girmeleri için küçük işletmeleri desteklemek amacını taşımaktadır.

Birleşik Arap Emirlikleri, merkezi ve yerel kamu varlıkları için topluluk bulut mimarisine dayanan bir kamu bulutu başlatmayı planlamaktadır. Bu plan kamu hizmetlerini iyileştirme, maliyetlerini azaltma ve kamu kurumları arasındaki işbirliğini artırma amaçlarını taşımaktadır (Zwattendorfer, 2013a).

2.2. Ülkemizde Bulut Bilişim

Ülkemizde özellikle 2000'li yılların başlarından itibaren gerek Avrupa Birliği uyum süreci çerçevesinde ve gerekse de özel sektör kuruluşlarının iş ve işlemlerinde sağladığı maliyet, zaman ve personel tasarruflarını dikkate alarak; kamu kurum ve kuruluşları bilgi teknolojileri alanında proje ve yatırımlara hız vermişlerdir. Bu proje ve yatırımların hız kazanmasında bu dönemdeki hükümetlerin düzenleyici strateji ve eylem planlarının etkisi büyüktür. Bu anlamda Avrupa Birliği tarafından başlatılan e-Europe+ girişimine paralel olarak 2002 yılında ortaya konulan e-Türkiye Girişimi Eylem Planı önem taşımaktadır.

Bu girişimle, ülkemizde bilgi toplumuna geçişin yapı taşlarının oluşumunun hızlandırılması, daha ucuz, hızlı ve güvenli internet erişimi, insan kaynağına yatırım ve internet kullanımının yaygınlaştırılması hedeflerine ulaşabilmek için; e-Eğitim, e-Devlet, e-Ticaret, e-Çevre, e-Sağlık ve benzeri konular başta olmak üzere birçok alt bileşen ile Türkiye'nin bilgi toplumu çalışmaları için taban oluşturmak ve yol göstermek hedeflenmiştir (e-Türkiye Girişimi Eylem Planı, 2002).

Yine bu girişimin devamında, 27 Şubat 2003 tarihinde yayımlanan 2003/12 sayılı Başbakanlık Genelgesi ile e-Dönüşüm Türkiye Projesi başlatılmıştır. Bu projenin başlıca hedefi; vatandaşlarımıza daha kaliteli ve hızlı kamu hizmeti sunabilmek amacıyla; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş bir devlet yapısı

oluşturacak koşulların hazırlanmasıdır (T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi, 2009). Bu projenin yürütülmesini sağlamak amacıyla 2003 yılında Kısa Dönem Eylem Planı ve 2005 yılında Eylem Planı hazırlanmıştır. 2005 Eylem Planının uygulanması sonrasında, 2005-2006 yıllarında Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanarak; 2006-2010 döneminde uygulanmak üzere 2006 yılı Temmuz ayında 2006/38 sayılı Yüksek Planlama Kurulu kararı ile yürürlüğe konulmuştur.

Bu Eylem Planında; kamuda ekonomik etkinliği azaltan diğer nedenlerin yanı sıra iş süreçlerinde etkinliğin sağlanamamasının, kamu tarafından yaratılan katma değerin düşük olmasının önemli bir nedeni olduğu belirtilmektedir. Yine, bilgi ve iletişim teknolojilerinin, iş süreçlerinde etkinliğin artırılması için önemli bir araç olarak ortaya çıktığı ve bu teknolojilerin sağladığı olanaklardan en üst düzeyde yararlanarak kamu iş süreçlerinde etkinliğin artırılması için; kurumlararası işbirliğinin geliştirilmesi, ortak altyapıların kullanımı, mükerrer yatırımların engellenmesi, bilgiye dayalı etkin karar alma süreçlerinin oluşturulması, nitelikli insan kaynağının ve örgütsel kapasitenin geliştirilmesi ve vatandaş odaklı, güvenilir, birlikte çalışabilir, bütünleşik ve etkin bir e-devlet yapısının kurulması gerektiği belirtilmektedir. Ayrıca ilgili Eylem Planında, verimliliği ve vatandaş memnuniyetini öncelikli olarak gözeten, ülke koşullarına uygun, örgüt ve süreç yapılanmalarına sahip etkin bir e-devlet oluşumunun bilgi ve iletişim teknolojileri desteğiyle hayata geçirilmesi, strateji olarak belirlenmiştir. Yakın gelecekte, kamu kurumları arasında işbirliği ve birlikte çalışabilirlik yeteneklerinin geliştirilmesi, kaynak israfının azaltılması, iş süreçlerinde verimliliğin artırılması ve bilgiye dayalı politika ve karar oluşturma süreçlerinin geliştirilmesinde, bilgi ve iletişim teknolojilerinin en önemli araç olacağı ve kamu bilgi ve iletişim teknolojileri alımlarında, açık standartların kullanımı ve yazılım kalite standartlarının uygulanmasıyla, özellikle yazılım ve hizmetler alanında bağımlılık oluşturarak rekabeti azaltan hususların giderileceği vurgulanmıştır (DPT Bilgi Toplumu Stratejisi, 2006-2010). Bu eylem planında ortaya konulan; internet çıkışları için ortak bir güvenli iletişim altyapısı kurularak e-devlet mimarisinin omurgasının oluşturulması, olağanüstü durum yönetim sistemi kurulması, kullanıcı ihtiyaçlarına göre gerektiğinde birleştirilerek ve

basitleştirilerek yeniden tasarlanabilecek iş süreçlerine sahip hizmetlerin; etkin, hızlı, sürekli, şeffaf, güvenilir ve bütünleşik şekilde sunumu, hizmetlere tek kapıdan ve farklı platformlardan ulaşılması, kamu kuruluşlarının internet sitelerinin merkezi olarak barındırılması, internet siteleri için görsel, hizmet kalitesi, içerik, güvenlik, kimlik yönetimi ve kullanılabilirlik standardizasyonunun sağlanması gibi birçok hedef, kamu kurum ve kuruluşlarının bulut mimarisine geçmelerinin temelini oluşturacak niteliktedir (DPT Bilgi Toplumu Stratejisi Eylem Planı, 2006-2010).

2013 yılında, Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 25. Toplantısında alınan 2013/104 sayılı karar uyarınca, kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir. Bu sayede yedeklilik, felaket kurtarma merkezi, siber güvenlik, iş sürekliliği, kamu bulutu, işletme maliyeti, kurumlar arası veri paylaşımı gibi hususların tamamına çözüm sağlanması amaçlanmaktadır. Bu karar Türkiye'nin bulut bilişim alanındaki çalışmalarına ivme kazandıran bir nitelik taşımaktadır.

2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı benzer şekilde, Kalkınma Bakanlığı Bilgi Toplumu Dairesi tarafından hazırlanarak 2015 yılında yayımlanan ve gelişen ve değişen bilişim teknolojilerine uygun şekilde bir devlet stratejisi ortaya koyan 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı'nda bulut bilişim teknolojileri ile ilgili fayda, tehdit, risk ve ayrıca kamusal hedeflere sıkça yer verilmiştir. Bu eylem planında bulut bilişim teknolojileriyle ilgili yer alan başlıca hedef ve stratejiler şunlardır:

- Türkiye'nin bölgesel veri merkezi olması ve bulut bilişimin yaygınlaştırılması,
- Başta KOBİ'ler olmak üzere işletmelerin iş verimliliğinin artırılmasında BT'den yararlanılması ve bu kapsamda bulut bilişim hizmetlerinin kullanımının desteklenmesi,

- Bulut bilişim hizmetlerinin gelişebilmesi ve yaygınlaşması için gerekli yasal ve idari düzenlemelerin yapılması,

- Hazırlanacak bir strateji doğrultusunda kamu bulutunun hayata geçirilmesi ve bu kapsamda, öncelikli olarak kamu veri merkezlerinin bütünleştirilmesi çalışmalarının tamamlanması, bulut bilişime ilişkin gerekli Ar-Ge çalışmalarının yürütülmesi, gerekli teknik, idari ve yasal altyapı oluşturularak ve kamu bulutu uygulama platformunun hayata geçirilmesi,

- KOBİ'ler için bulut programı geliştirilmesi,

- Kent Yönetimi Bilgi Sistemi geliştirilmesi kapsamında bulut bilişim hizmet sunum imkânlarının değerlendirilmesi,

- Kamu bulutuna 30 kurumun dâhil edilmesi,

- Kamu bulut bilişim altyapısının oluşturulması (DPT Bilgi Toplumu Stratejisi Eylem Planı, 2015-2018).

Son maddede yer alan kamu bulut bilişim altyapısının oluşturulması hedefi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından, TÜBİTAK, TÜRKSAT, TSE işbirliğiyle, öncelikle veri merkezlerinin bütünleştirilmesinden başlanarak gerçekleştirilecektir. 2018 yılında bitirilmesi planlanan projenin uygulama adımları şu şekilde sıralanmaktadır:

- Kamu bulutuna ilişkin yasal ve idari düzenlemeler hayata geçirilecektir. Bu kapsamda, kamu kurumları tarafından bulut bilişim altyapısının kullanımına yönelik usul ve esaslar, bulut bilişimin farklı hizmet seviyeleri ve sanallaştırma hizmeti için belirlenecektir.

- Bulut bilişim altyapılarında kullanılan sanallaştırma, ince istemci gibi çözüm ve teknolojiler değerlendirilecek, önceliklendirilecek ve bu önceliklendirmeye göre;

ilgili konularda Ar-Ge çalışmaları yürütülerek, çözüm ve teknolojiler hayata geçirilecektir. Kurulan altyapıların felaket kurtarma merkezi olarak kullanılması hususunda gerekli yaptırım ve teşvik mekanizmaları hayata geçirilecektir.

- Servis olarak Yazılım seviyesinde, kamu genelinde yaygınlaştırılması planlanan öncelikli bulut bilişim uygulamaları tespit edilerek bu uygulamalar geliştirilecek, tanıtımı yapılacak ve yaygınlaştırma çalışmaları yürütülecektir.

- Servis olarak Platform seviyesinde, bulut bilişim altyapısı üzerinde çalışacak ve üzerinde uygulama geliştirilmesine imkân tanıyacak ara katman yazılımı geliştirilecek ve gerekli eğitimlerin verilebileceği bir mekanizma tasarlanarak hayata geçirilecektir.

- Altyapı ve uygulama yazılımlarında açık kaynak kodlu yazılımlara öncelik verilecektir.

- Bulut bilişim için gerekli destek programları planlanarak uygulamaya konacaktır (DPT Bilgi Toplumu Stratejisi Eylem Planı, 2015-2018).

2016 yılı BSA Puan Çizelgesinde Türkiye, 24 öncü BT ekonomisi arasında 19. sıraya yerleşmiştir. 2013 senesinde sahip olduğu 18. sıra ile karşılaştırıldığında, Türkiye'de bulut bilişim ile ilgili yasal ve düzenleyici çerçeve konusundaki çalışmaların hızlandırılmasının gerekliliği görülmektedir.

Ülkemizin gelişen bilişim teknolojilerine uyum sağlamaktaki kararlılığı ve bu doğrultuda yaptığı çalışmalar neticesinde, birçok kamu kuruluşu günümüz bilişim dünyasının gözdesi haline gelen bulut bilişim konusunda projeler geliştirmiş ve geliştirmeye devam etmektedir. Bu bağlamda ülkemiz genelinde kamu kuruluşlarında mevcut kullanılan bulut bilişim ve/veya bulut bilişim benzeri yapılar olarak başlıca; Adalet Bakanlığı-Ulusal Yargı Ağı Projesi, Maliye Bakanlığı-Kamu Harcama ve Muhasebe Bilişim Sistemi, Sosyal Güvenlik Kurumu-Özel Bulut Teknolojileri Projesi, İçişleri Bakanlığı-Merkezi Nüfus İdaresi Sistemi, TÜRKSAT-Ulaştırma, Denizcilik ve

Haberleşme Bakanlığı-Ulusal Ulaştırma Portalı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Kıyı Emniyeti Genel Müdürlüğü-Uzak Mesafede Gemilerin Takibi Projesi Felaket Kurtarma Merkezi, Tapu ve Kadastro Genel Müdürlüğü-Veritabanı Yedeklemesi, İçişleri Bakanlığı Mahalli İdareler Genel Müdürlüğü-Yerel Bilgi Portalı ve Tübitak-Ulaknet Veri Merkezi sıralanabilir. Sıralanan bu bulut bilişim ve/veya bulut bilişim benzeri hizmetlerin bir çoğu lokal ölçekli, belli bir Bakanlığın veya Genel Müdürlüğün uygulamalarını servis edebilmesi ve/veya iç hizmet akışını yürütebilmesi amacıyla oluşturulan yapılardır.

Yine Aile ve Sosyal Politikalar Bakanlığı tarafından tamamlanan, Bulut Sanal Veri Merkezi ve Sosyal Yardım Bilgi Sistemi projeleri Türkiye'de kamusal alanda bulut bilişime geçişte önemli kilometre taşlarından biridir. Başbakanlığa bağlıyken ilgili Bakanlık çatısı altında toplanan kurumların bilgi işlem birimlerinin birleştirilmesi sebebiyle, bilgi işlem altyapılarının da entegre edilmesi gereksinimi sonucu ortaya çıkan pojeyle; 320 adet sanal sunucu ile toplam 25.000 son kullanıcıya hizmet verebilecek şekilde 5 adet sistem odasından oluşan bir entegre veri merkezi kurulmuştur. Bu amaçla, aile bulutu dönüşümü için 100'ün üzerinde sunucu özel sanal veri merkezine aktarılmıştır. Söz konusu aktarım sırasında sanal ortama doğrudan aktarılamayacak risk tabanlı işlemcilere sahip sunucular, öncelikle sanal ortamda çalışabilecek işletim sistemlerine çevrildikten sonra ilgili aktarımlar gerçekleştirilmiştir. Bu bağlamda, kurumsal veri ve uygulamaların Saklama Alanı Ağı (Storage Area Network (SAN)) depolama üniteleri üzerinde saklanması sağlanmış ve SAN Depolama ürünlerini daha verimli kullanmak için Tekilleştirme (Deduplication) ve Depolama Sanallaştırma (Thin Provisioning) özellikleri kullanılmıştır. Sunucu ve ağ bağlantılarına 10 GBit hızında iletişim altyapısı sağlanmıştır. Canlı sistem ve yedekleme için gerekli ağ bağlantıları, ağ teknolojileri kullanılarak biribirinden tamamen ayrıştırılmıştır. Tüm yapı yedekli ve iş sürekliliğini sağlayacak şekilde projelendirilmiştir (Ergin, 2012).

Ülkemizde kamu bulutları kurulması ve yaygınlaştırılması amacıyla başlatılan önemli projelerden biri de İçişleri Bakanlığı Bulut Belediye Projesi'dir. Bu projedeki genel amaç, bilgi işlem birimi olmayan veya kısıtlı imkânlar nedeniyle bilgi

teknolojilerinden yeterince faydalanamayan küçük ve orta ölçekli belediyelerin bu alandaki ihtiyaçlarının karşılanması ve vatandaşa daha etkin ve hızlı bir hizmet sunumu yapabilmelerinin sağlanmasıdır (T.C. İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı, 2014).

Bu proje ile;

- Pilot olarak seçilen ve bilgi işlem birimi olmayan küçük ve orta ölçekli 20 belediyenin, iş ve işlemlerinin merkezi bir yapı ile elektronik ortamda yürütülmesi,
- Belediyelerin Bulut Belediye sistemi içinde ihtiyaç duyacakları merkezi veri tabanlarından (MERNİS, AKS, TAKBİS, POLNET, UYAP, SGK vb.) anlık ve kesintisiz yararlanmasını sağlamak amacıyla gerekli altyapının oluşturulması,
- Uygulama altyapısının standardize edilerek farklı paket programların kullanımının önlenmesi,
- Belediyelerin iç işleyişine yönelik; meclis ve encümen kararları, muhasebe, bütçe, emlak, personel, taşınır mallar vb. modüllerin geliştirilmesi,
- Merkezi idarelerin, belediyelere ilişkin ihtiyaç duyduğu verilerin üretilmesi,
- Vatandaşın belediye hizmetlerinden elektronik ve/veya mobil imza ile yararlanmasına olanak sağlayacak altyapının oluşturulması,
- 7/24 yerel hizmet sunumu,
- Alt yapı düzenlemesi sağlanması,
- Bankalar ile anlık veri transferi sağlanarak, vatandaşların vergi ve fatura gibi ödemelerinin online olarak yapılmasının sağlanması,

- Belediye-Vatandaş ilişkisinin daha etkileşimli bir zemine taşınması amaçlanmaktadır.

Bu kapsamda, İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığının sorumluluğunda; Kalkınma Bakanlığı, Çevre ve Şehircilik Bakanlığı, Türkiye Belediyeler Birliği ile belirlenen belediye ve özel sektör temsilcilerinin katılımıyla, 23 Eylül 2014 tarihinde '1. Bulut Belediye Projesi Çalıştayı' düzenlenmiştir. Çalıştayda belediyelerin projeden beklentilerine, projeye yönelik önerilerine, diğer Bakanlık ve kamu kurumları ile özel sektörün projedeki rolüne ve görevlerine, projenin uygulama adımlarına ve yol haritasının belirlenmesine yönelik karşılıklı fikir paylaşımında bulunulmuştur (T.C. İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı, 2014).

Bakanlığımızca yürütülen CBS Altyapısının Kurulması ve Geliştirilmesi projesi, ülkemizde bulut bilişim mimarisinin tesis edilmesi amacı doğrultusunda geliştirilen ve uygulanan öncü projelerden birisidir. Bu proje ile, Bakanlık bilişim alt yapısının entegre bir şekilde çalışabilmesi için gerekli asgari ihtiyaçların sağlanması ve bulut mimari ile tasarlanan bu alt yapının gelecekte Kamu Entegre Veri Merkezi altyapısıyla entegrasyonunun mümkün kılınması planlanmıştır. Yine kurulan bilişim alt yapısı üzerinde, öncelikli olarak CBS yazılımlarının, Servis olarak Yazılım (SaaS) modeliyle oluşturulması ve bu yazılımların düşük maliyet ile standart bir yapıda servis edilerek yaygınlaştırılması hedeflenmiştir.

2016 yılı sonunda tamamlanan projeyle, öncelikle kritik e-devlet projelerinin bu mimari üzerinden servis edilebilmesi amacıyla, kuruma ait tüm bilişim kaynakları merkezi bir yapıya taşınmıştır. Bu kapsamda temin edilen IBM Pure Application donanım ve yazılımı ile Bakanlığa ait özel bulut mimarisi kurulmuştur. Bu altyapı gerektiğinde Bakanlığın hibrit bulut mimarisine geçebilmesi ve diğer kamu veya özel sektör bulut altyapılarıyla entegre çalışabilmesine imkân verebilecek niteliktedir. Kurulan bu entegre bilişim altyapısı sayesinde sanallaştırma en üst düzeye çıkarılarak ve belli hizmetler için tahsis edilmiş bilişim kaynakları (sunucu, depolama ünitesi vb.) tek

bir altyapıda toplanarak, kaynakların atıl vaziyette durmasının önüne geçilmiştir. Yine bu altyapı sayesinde kuruma:

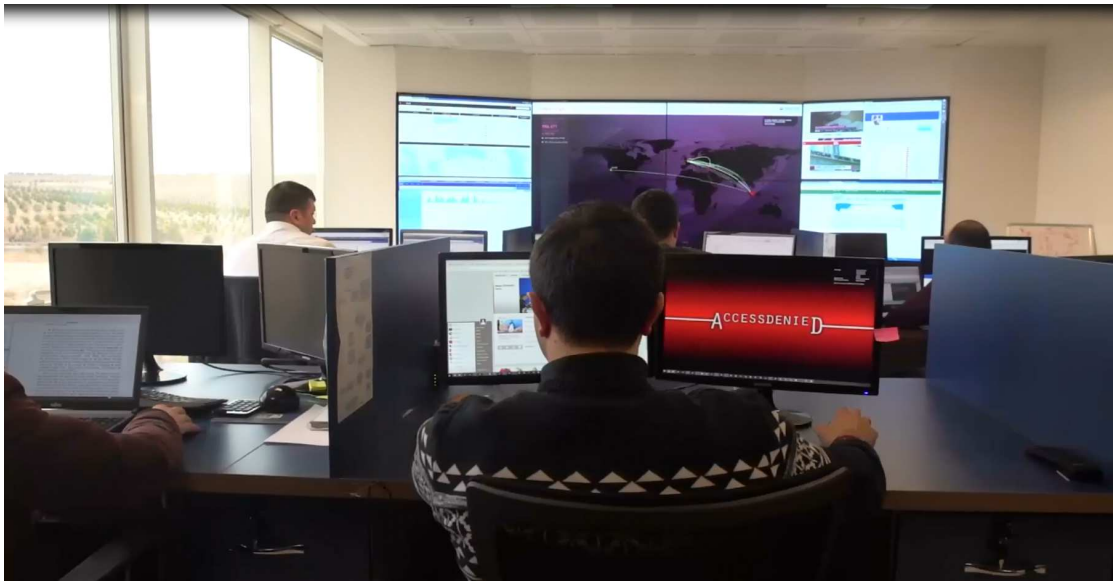
- Fiziksel kaynakların bulut mimarisindeki gruplara kolayca paylaştırılabilmesi ve izolasyonu,
- Ani kullanım artışlarında bilişim kaynaklarının otomatik ve dikey ölçeklendirilebilmesi,
- Uygulama güvenliğini arttırmaya yönelik olarak uygulama şablonları için entegre şifreleme desteği,
- Kurumun kullandığı iç ve dış yazılımlar için lisans yönetimi özelliği sayesinde geliştirilmiş yönetişim,
- Geliştirilmiş yedekleme, geri yükleme ile yüksek kullanılabilirlik avantajları sağlanmıştır.

Ayrıca yine bu altyapı üzerinde çalışan IBM Cloud Orchestrator yazılımıyla, Bakanlık özel bulutunun yönetilmesi ve Bakanlık kullanıcılarınca ihtiyaç duyulan donanım ve yazılımların geleneksel mimariye göre çok daha hızlı bir şekilde temini sağlanmıştır. Bu yazılım açık, özel ve hibrit bulutların yönetilmesi için gerekli menü ve özelliklere sahip olup; sistem bileşenleriyle ilgili yapılandırma, tahsis ve devreye almanın kolay bir şekilde gerçekleştirilmesine imkân tanımaktadır. Yine bu yazılım yoluyla ölçüm, kullanım, muhasebe, izleme ve kapasite yönetimi gibi yönetim araçları bulut hizmetleriyle bütünleştirilebilmektedir.

Resim 2.1: Çevre ve Şehircilik Bakanlığı Veri Merkezi

İlgili CBS Altyapısının Kurulması ve Geliştirilmesi Projesi, kurulan entegre sistem altyapısı ve özel Bakanlık bulutu haricinde, kurulan sistemin güvenli ve verimli bir şekilde yönetilmesini ve idamesini sağlamak amacıyla; kimlik yönetimi altyapısının kurulması, siber güvenlik altyapısının kurulması, bulut dosya depolama ve paylaşım platformunun oluşturulması gibi önemli proje bileşenleri de içermektedir. Bu haliyle farklı sistem ve altyapıların aynı proje ile temini yoluyla; bu sistem ve altyapıların birbiriyle bütünleşik çalışabilmesi sağlanmış ve doğabilecek muhtemel sistem uyumsuzluklarının önüne geçilmiştir.

Siber Güvenlik altyapısının kurulması iş paketiyle, Bakanlığımızda Siber Güvenlik Operasyon Merkezi kurulmuş, Saldırı Önleme Sistemi temin edilmiştir. Yine ilgili Siber Güvenlik Operasyon Merkezinin ve Saldırı Önleme Sisteminin yönetimi için gerekli danışmanlık hizmetleri ve eğitimler alınmıştır.



Resim 2.2: Çevre ve Şehircilik Bakanlığı Siber Güvenlik Operasyon Merkezi

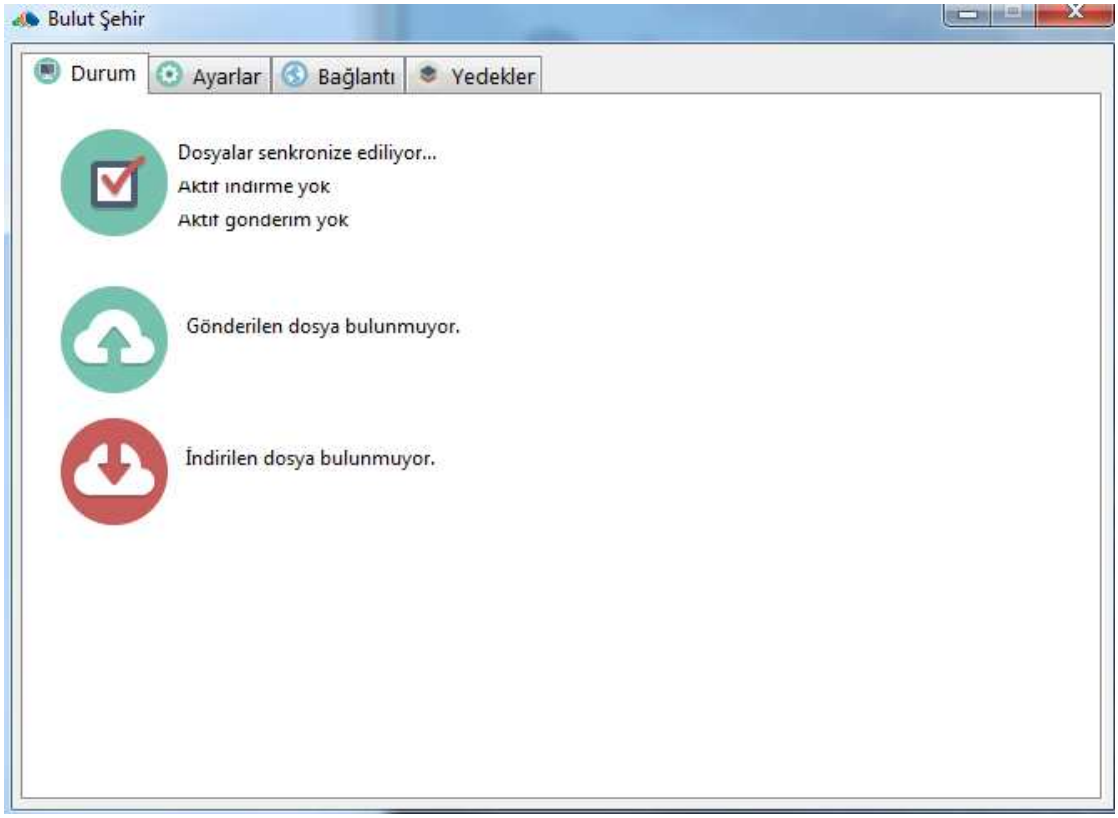
Yine bu proje kampsamında gerçekleştirilen Kimlik Yönetimi altyapısının kurulması iş paketiyle, Bakanlık kullanıcılarının, Bakanlığın farklı uygulamalarına tek bir kullanıcı kimliği ile erişiminin sağlanması için gerekli altyapı oluşturulmuş ve ilk etapta Bakanlığımızın 12 adet uygulaması bu altyapıya taşınmıştır. Yine kimlik yönetimi altyapısı sayesinde tüm kullanıcılara rol, görev ve yetki tanımlarının tek elden yapılarak, sadece kendilerine tanımlanan rol, görev ve yetkiler kapsamında ilgili uygulama ve portalları kullanmaları sağlanmıştır. Ayrıca kullanıcı kimlik tanımlama (kullanıcı adı, şifre) kuralları geliştirilerek, farklı uygulamaların önüne geçilmiştir.

Bu proje kapsamında geliştirilen ve Bakanlıklar düzeyinde bir ilk olma özelliği taşıyan diğer bir iş paketi Bulut Şehir Dosya Depolama ve Paylaşım Platformudur. Bu platform günümüzde çok sık kullanılan Google Drive, Dropbox, One Drive vb. dosya depolama ve paylaşım platformlarının sağladığı, platform ve lokasyon bağımsız olarak dosya erişim ve paylaşım özelliklerini Bakanlığımızın tüm kullanıcılarına sunmaktadır. Bu platform masaüstü, web ve mobil arayüzleri sayesinde; tüm verilere platform bağımsız bir şekilde ev, ofis bilgisayarlarından, tablet ve cep telefonlarından ve web tarayıcısı olan her türlü diğer cihazdan erişim sağlama ve internet erişimi bulunan her

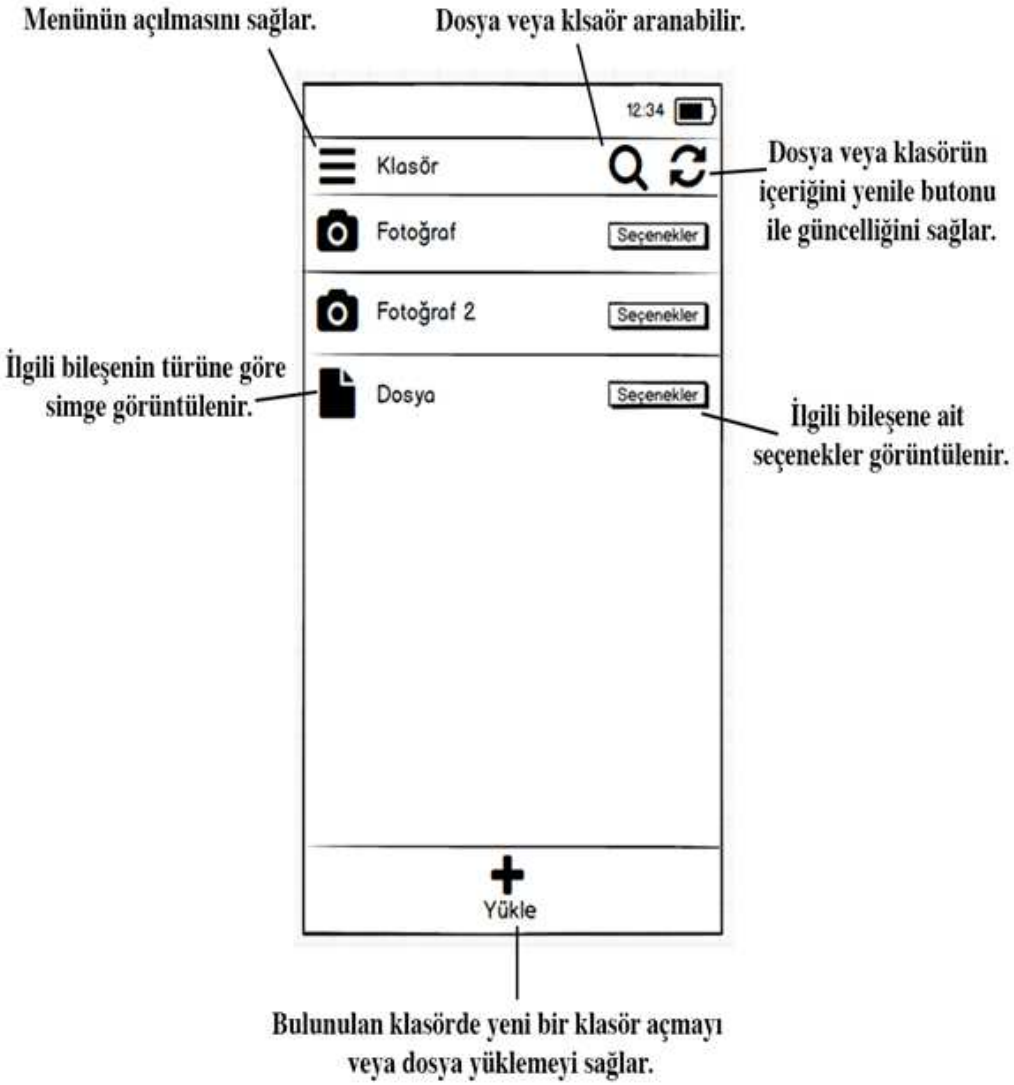
yerden bu verileri kullanma ve paylaşma imkânı sağlamaktadır. Herhangi bir arayüze yüklenen veri, diğer arayüzlerde otomatik olarak senkron olmaktadır. Yine kullanıcılar arasında açılan paylaşım klasör ve bunların içindeki dosyalarda yapılan tüm değişiklikler senkronizasyonla, tüm paydaşların tüm platformlarına otomatik olarak yansımaktadır.

Resim 2.3: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Web Giriş Arayüzü

Resim 2.4: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Web Arayüzü



Resim 2.5: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Masaüstü Arayüzü



Şekil 2.1: Çevre ve Şehircilik Bakanlığı Bulut Şehir Dosya Depolama ve Paylaşım Platformu Kullanıcı Mobil Arayüzü (Android)

Güvenli dosya depolama ve paylaşımı ile kurumda birlikte çalışılabilirliği önemli düzeyde artıran platformdaki tüm veriler, kurumun veri merkezinde bulunan özel bulut

altyapısında şifreli bir şekilde saklanmaktadır. Kullanıcılar diğer kullanıcılarla dosya paylaşımına ek olarak, kurum dışındaki kullanıcı olmayan kişilere link paylaşımı yoluyla dosyalar gönderebilmektedir. Ayrıca yedekleme özelliği sayesinde kullanıcılar masaüstündeki istedikleri dosyanın yedeğini platformda oluşturarak tutabilmektedirler.

Özetle CBS Altyapısının Kurulması ve Geliştirilmesi projesiyle; Bakanlığımızın sahip olduğu bilişim kaynaklarının tek bir altyapıda toplanarak esnek, erişilebilir ve kullanılabilir şekilde iç ve dış kullanıcılara hizmet vermesinin sağlanması, gerek e-devlet uygulamalarımızın ve gerekse de vatandaşlarımıza ve ihtiyaç duyan kuruluşlara hizmet veren diğer uygulamalarımızın bu altyapı ile platformdan bağımsız olarak güvenli şekilde sunulabilmesi ve uzun vadede kurulacak Kamu Entegre Veri Merkezi altyapısıyla entegrasyonun kolayca sağlanması amaçlanmaktadır. Daha önce de bahsedildiği üzere, e-devlet konusunda öncü bazı ülkeler, geleneksel mimariye uygun şekilde geliştirilmiş uygulamalarını bulut bilişim mimarisine taşımakta zorluklar yaşamakta ve bu durum ilgili ülkelerin bulut bilişime geçişlerini zorlaştırarak, kamu sektörlerinin bulut bilişim alanında göreceli olarak geri kalmalarına sebebiyet vermektedir. Bu sebeple, özellikle e-devlet hizmetleri açısından bakıldığında, gelecekte bulut bilişim altyapısında çalışacak ilgili hizmetlerin, geleneksel bilişim mimarilerine uygun şekilde kurulup yaygınlaşmasından önce, kamu bilişim altyapısının bulut mimarisine uygun hale getirilerek; geliştirilecek projelerin bu altyapıya uygun şekilde geliştirilmesi gerekmektedir. Bu şekilde ileride atıl duruma düşecek birçok yazılım ile ilgili maliyetin de önüne geçilmiş olacaktır.

Sonuç olarak ülkemizde bulut bilişim veya benzer mimarilerin kullanılması amacıyla birçok kurum ve kuruluş çeşitli çalışmalar yapmaktadır. Bu çalışmaların ileride tek bir ortak altyapının kullanılması ve oluşturulacak kamu bulutlarının birbirleriyle entegre bir şekilde çalışması hedefleriyle; belli standartlar çerçesinde gerçekleştirilmesi önem taşımaktadır. Ayrıca ülkemizde veri gizliği ve güvenliği, haberleşmenin ve özel hayatın gizliliği, veri paylaşımı ve kişisel verilerin korunması ve bulut bilişim sağlayıcı ve hizmet standartları gibi konularda mevzuata ilişkin gerekli çalışmaların yapılması ihtiyacı öne çıkmaktadır.

2.3. Entegre Kamu Hizmetleri İçin Gereksinimler ve Bulut Çözümleri

2000'li yıllarda internetin yaygın olarak kullanılmaya başlamasıyla birlikte vatandaşların internet ortamında her geçen gün daha fazla vakit geçirmeleri, öncelikle özel sektörün ve hemen ardından kamu sektörünün dikkatini çekmiş ve hemen bütün iş kollarında faaliyet gösteren kuruluşlar, sundukları hizmetleri mümkün olduğunca internet ortamına taşıyarak, yer ve zaman bağımsız olarak vatandaşların belli hizmetlerden faydalanabilmelerini sağlamayı ana hedef olarak belirlemişlerdir. Kamu kuruluşlarının internet üzerinden oluşturdukları platformlar vasıtasıyla hizmet sunmaya başlamaları e-devlet kavramının doğmasını sağlamıştır. Tanım olarak e-devlet, kamuda hizmet sunumunun verimlilik ve etkinliğini geliştirmek ve/veya artırmak için, Bilgi ve İletişim Teknolojileri (BİT'ler) ve diğer web tabanlı telekomünikasyon teknolojilerinin kullanımıdır (Hai, 2007).

Ancak zamanla bilişim teknolojilerinde meydana gelen önemli gelişmeler, merkezi ve yerel kamu kuruluşları için e-devlet hizmet modelinin yetersiz kalmasına sebep olmuş ve İngilizce "Connected Government" (c-government) veya "Government 2.0" kavramları ortaya çıkmıştır. Bu bölümde entegre kamu hizmetleri için bu yeni hizmet modeli c-devlet olarak adlandırılacaktır.

C-devlet; kamu kuruluşlarının, vatandaşların ve yenilikçi şirketlerin şeffaflık ve verimliliklerini artıracak bir açık kaynak bilişim platformu oluşturmak için, ortak çalışmaya dayalı teknolojilerin kullanılmasını amaçlayan devlet politikalarını temsil eder (O'Reilly, 2009).

C-devlet, Web 2.0 esaslarıyla e-devleti birleştirir ve yenilikçi uygulamalar, web siteleri ve widgetların gelişmesini sağlayan açık kaynak platformları kullanarak vatandaşın katılımını artırır. Devletin rolü bir altyapı olarak açık verileri, web hizmetlerini ve platformları sağlamaktır (Howard, 2012).

Özetle e-devlet, kamu hizmetlerinden faydalanan vatandaşların ve kuruluşların hizmet tedarik koşullarını iyileştirmek ve devletin verimliliğini artırmak için, bilgi ve

iletişim teknolojileri (BİT) ve yeni ortaya çıkan diğer teknolojilerin kullanımıdır. Bu sayede kamu kuruluşlarınca kazanılan organizasyonel beceriler, kamu hizmetlerini ve bu hizmetlerin üzerine kurulduğu süreçleri iyileştirerek; kamu politikalarına olan desteği güçlendirir. C-devlet ise, bu amaçları bir adım daha ileri götürüp; bulut bilişim, mobil ve sosyal medya teknolojileri gibi yeni teknolojiler aracılığıyla, devlet ve vatandaşlar arasındaki etkileşimi daha da artırmayı sağlar. E-devletin ilk yıllarında sadece web siteleri ve portalları aracılığıyla vatandaşa genel bilgi sağlanması olan işlevi, gelişim sürecinde vatandaşların yüksek düzeyde etkileşim sağlayarak; kamu uygulama, karar ve süreçlerini etkilemesine imkân sağlayan bir noktaya ulaşmıştır. Ulaşılan bu noktada daha esnek, yüksek performansa sahip, işbirliğine açık teknolojilerin kulanılmaya başlanması, c-devlet hizmet modelinin gelişmesi sonucunu doğurmuştur. E-devlet ve c-devlet modellerinin teknoloji, strateji ve hizmet odak noktası yönleriyle karşılaştırılmasına Tablo 2.2'de yer verilmiştir.

	E-Devlet	**C-Devlet**
Teknoloji	Statik, İnternet, Domaine özgü, Web 1.0	Vatandaş odaklı, Sosyal medya, Mobil, Web 2.0
Strateji	İçten dışa, Devleti esas alan	Dıştan içe, Vatandaşı esas alan
Hizmet Odak Noktası	Pasif faydalanıcılar olarak vatandaşlar	Aktif katılımcılar olarak vatandaşlar

Tablo 2.2: E-Devlet ve C-Devlet (Kaynak: Khan and Swar (2013))

2.3.1. Entegre Kamu Hizmetleri İçin Gereksinimler

Kamu hizmetlerinin daha verimli ve etkin sunumu ve ayrıca ortaya çıkan c-devlet hizmet modelinin uygulanabilirliğinin artırılması için; bulut bilişim teknolojileri

ve dış kaynak kullanımı yoluyla vatandaşların hizmet taleplerinin tek çatı altında toplanması gerekmektedir. Bu sayede vatandaşlar internet ortamında fazlaca vakit kaybetmeden ihtiyaç duydukları hizmet sunucusuna erişebilme, kullanacağı hizmet hakkında bilgi edinebilme ve standart bir şekilde işlemini gerçekleştirebilme imkânına kavuşacaktır.

Türkiye'de e-devlet platformunun sağlanmasından sorumlu olan T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na ait e-devlet portalında, Türkiye'de e-devletin genel görünümüyle ilgili; hizmetlerin ortak standartlara dayalı olarak, alanında uzman bilişim personelinin gözetiminde, mümkün olduğunca birleştirilmiş altyapılar üzerinden ve kamu kuruluşlarının birbirleriyle güçlü etkileşimi ve sundukları hizmetlerin entegrasyonunun sağlanarak sunulmasının önemi ortaya konulmaktadır.

Türkiye'deki e-devlet çalışmaları, başlangıçta bütüncül bakış açısı yerine kurumsal düzeydeki yaklaşımlarla gerçekleştirilmiştir. Hayata geçirilen sistemlerin geliştirilmesinde çoğunlukla kurumların sadece kendi ihtiyaçları ve sundukları hizmetler dikkate alınmıştır. Bu yaklaşımlarla geliştirilen sistemlerin birbirleri ile veri paylaşım ihtiyacı ortaya çıktığında, sorunlar yaşanmaya başlanmıştır. Türkiye'de kamu kurum/kuruluşlarının e-dönüşüm olgunluk düzeylerinde farklılıklar olduğu görülmektedir. Bu farklılıkların ortaya çıkmasındaki en büyük etken, e-devlet çalışmaları için gerekli nitelikli insan kaynağının istihdam edilmesinde yaşanan zorluklardır. Kamu kurum/kuruluşları e-devlet projelerini kendi imkânları ve insan kaynağı ile yürütmeye çalıştıkları için; bu projelerin planlamasında ve hayata geçirilmesinde sorunlar yaşanabilmekte, farklı yetkinliklerde veya mükerrer çözümler üretilebilmektedir. E-devlet çalışmalarının hem kurum içinde hem de kurumlar arasında bütüncül bir şekilde yürütülmesi ve koordine edilmesine yönelik bir organizasyon modeline ihtiyaç duyulmaktadır.

Kamudaki bilgi sistemlerinin bir e-devlet mimarisi genel çerçevesinde şekillendirilmemesi nedeniyle; güvenlik riskleri başta olmak üzere, sistemlerin birbirleriyle konuşamaması, hizmet kalitesinin düşmesi, aynı verilerin defalarca farklı

sistemlerde tutulması gibi pek çok sorun yaşanmakta ve gereksiz maliyetler oluşmaktadır. Her kurum kendi ihtiyaçları doğrultusunda BT altyapılarını ve bilişim sistemlerini hazırlamaktadır. Farklı kurumlar tarafından benzer ihtiyaçları karşılamak için mükerrer yatırımlar yapılabilmektedir. Elektronik veri ve belge paylaşımı, elektronik kimlik kartı, merkezi kimlik doğrulama altyapısı ve kamu ağı gibi birçok başlık bir kamu kurumu/kuruluşunun doğrudan hizmet alanında yer almayıp, tüm kurum/kuruluşların faydalandığı ortak altyapılardır. Ancak mevcut durumda kamu kurum/kuruluşları bu alanlarda ayrı ayrı çalışmalar yapmaktadır. Ortak altyapıların olmaması aynı zamanda kamu kurum / kuruluşlarının birlikte çalışabilirliğini de zorlaştırmaktadır.

E-devlet hizmet sunumunda ortak yaklaşımların olmaması, hizmet olgunluklarının da birbirinden farklı düzeylerde bulunmasına sebep olmaktadır. E-devlet hizmetleri kamu kurum/kuruluşları tarafından çoğunlukla birbirleri ile entegrasyon sağlanmadan bağımsız bir şekilde sunulmakta ve bütüncül süreçler işletilememektedir. Ayrıca kurumlar arası sistem entegrasyonlarının sağlanmasında idari ve teknik aksaklıklar yaşanması, entegrasyonların istenilen seviyede olmaması ve gerekli mevzuat düzenlemelerinin yapılamaması/eksik olması kurumlar arası veri paylaşımının önünde önemli engeller olarak durmaktadır (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016).

Yukarıda bahsedilen hususlar ülkemizde her kurum veya kuruluşun kendi veri merkezlerini işletmesi ve kendi hizmetlerini kendi platformlarından servis etmesinin yol açtığı zorluk ve engellerden sadece bazıları olup diğerleri şu şekilde sıralanabilir:

BT ekipman temini ve bakımı birçok kamu kuruluşunun uzmanlık alanı değildir. Bu sebeple ihtiyaç duyulan BT altyapısının yetersiz seviyede sağlanması ve bakımının uygun şekilde yapılmaması, ekipmanların yükünün ve etkin kullanım düzeylerinin yeterli izlenememesi, veri yedekleme ve felaket kurtarma sistemlerinde kısmi uygunsuzluklar yaşanması sorunlarıyla sıkça karşılaşılmaktadır.

Kamu kurumları, mevcut bilgi sistemlerinin işletilmesi ve idamesi için gerekli; sunucu, ağ ve bağlantı cihazları vb. ekipmanların tedariği için gerekli ödemeleri yıllık bütçelerinden karşılarlar. Geliştirilen yeni uygulama ve servisler için daha fazla kaynağın gerektiği durumlarda, ilgili bilişim kaynağının temini uzun süreli ek alım prosedürleri gerektirecek ve bu durum her bir kamu kuruluşu için ayrı ayrı hizmet sürecinin yavaşlamasına yol açabilecektir.

Aynı şekilde satın alınan yazılım fonksiyonlarının kuruluşların tüm gereksinimlerini karşılamaması halinde, bu yazılım çözümlerinin iyileştirilmesi /geliştirilmesi için ek bütçe kaynaklarını sağlamak zorunda kalırlar. Bu da hem maliyet hem de iş süreçlerinde artışa neden olur.

Bugün, birçok devlet kurumu donanım ve yazılım satın alarak, veri merkezleri oluşturarak ve hizmetlerinin otomasyonu yoluyla, vatandaşlara hizmetler sunmaktadır. Bu durum her kuruluşun; altyapı, danışmanlık hizmetleri, fizibilite çalışmaları, yazılım geliştirme, ekipman alımı, lisans, bakım için ayrı ayrı ihale ve sözleşme yapması ile birlikte bu işlerin ilgili denetleyici devlet kurumlarının denetiminden geçmesi sonucunu doğurmaktadır. Bu durum hem aşırı bir iş yükü oluşturmakta ve hem de küçük ölçekli alımlar için ayrı ayrı yapılan harcamalar maliyet etkin olmaktan uzak kalmaktadırlar.

Ayrıca, genel olarak kamu kurumları ihtiyaç duyduklarından çok daha fazla miktarda bilgi ve iletişim varlığına sahiptirler. Tedarik edilen donanım ve özellikle de yazılım çözümlerinin önemli bir kısmı, amacına göre veya uzun vadeli kullanılmaz. Bu durum, kamuda önemli miktarda bilişim kaynağının atıl kalmasına ve satın alınan veya geliştirilen birçok uygulamanın verimli bir biçimde kullanılamaması nedeniyle, boş yere harcama yapılmasına sebebiyet vermektedir.

Sıralanan bu sebepler, ülkemizde e-devlet ve bilişim hizmetlerinin bulut platformlarıyla tek çatı altından sağlanmasının ve bu hizmetlerin sunumu ve kamu kuruluşlarının iç bilişim ihtiyaçları için gerekli kaynak altyapısının, ortak veri merkezlerinde toplanmasının önemini ortaya koymaktadır. Bu bağlamda kamu entegre veri merkezleri ve kamu bulutları kurulması kaçınılmaz bir hal almaktadır.

Kamu bulutları, devlet kurumlarına hizmet vermek amacıyla temin edilen, bulut bilişim teknolojilerinin kullanan donanım ve yazılım paketleridir. Bilişim kaynaklarının kiralanması, yazılım ve ekipman temini ve yine bilgi iletişim teknolojileri aracılığıyla sunulan hizmetlerin, entegrasyonu ve haberleşebilmesi amacıyla uygulanan hizmet modelleridir.

Kamu bulut platformları kurulurken dikkat edilmesi gereken hususların başında, söz konusu platformların sanal ve bulut altyapılarının geliştirilmesi ile ilgili, alanında lider çözümler sunabilmesi gelmektedir. Ayrıca, kamu kurumlarının mevcut veri merkezlerinin buluta hızlı bir şekilde transferine olanak sağlamalıdır. Platformlar; yüksek kullanılabilirlik, veri kurtarma, sıcak (hizmet kesintisi olmadan) aktarım, sıcak kaynak eklemesi, esneklik, kaynakların otomatik dağıtımı, seri portlar için sanal hub ve API arayüzleri mağazası gibi olanaklar sunmalıdır.

Platform uygulamaları, mevcut altyapının entegrasyonunu ve kamu kuruluşlarının BT ekipmanlarının optimizasyonunu sağlamalıdır. Ayrıca, sunulan hizmetlerde operasyon sürekliliği ve acil kurtarma sağlanmasına ilişkin çözümler için, esnek ölçeklemeye imkân vermeli ve maliyetleri azaltmalıdır.

Platform ek modüller kurulumu yoluyla yatay ve dikey yönde genişleme imkânı sunarak, sanal veri merkezlerinde kaynakların birleşmesini sağlamalıdır. Veri merkezlerinde barındırılan uygulama ve hizmetler, tam otomatik web portalları ve yazılım arayüzleri yoluyla kullanıcılara sunulabilmelidir. Bunun yanında platform, yeni uygulamaların geliştirilmesi veya mevcut uygulamaların revizyonları için; geliştirme, test ve işletme ortamlarını desteklemelidir.Ayrıca kamu bulut platformları için diğer gereksinimler şu şekilde sıralanabilir:

- Sanal makinelerin (OVF) depolanması ve dağıtımı için açık standart desteği,
- Dış sistemlerle entegrasyon için açık yazılım arayüzü,
- Sanal makinelerin ve uygulamaların kurulması için klonlama kullanılabilme desteği,

- Depolama sistemine disk alanı sağlamak ve uygulamaların yüklenmesini optimize etmek için, entegre sanal makine kopyalarını destekleme,
- Gömülü sanal altyapı ağ güvenliği özellikleri,
- Altyapı hizmetleri katalog desteği,
- Sabit servis kalitesiyle, veri merkezleri üzerindeki sanallaştırma platformu tarafından sağlanan kaynak havuzlarının mantıksal bölümlenebilmesi,
- Çeşitli organizasyonlar ile işbirliği desteği, sanal kaynak izolasyonu, bağımsız LDAP kimlik doğrulaması,
- Kullanıcıların ve yöneticilerin erişimi için self-servis portal,
- Kuruluşların altyapılarının bağımsız yönetimi için geliştirilmiş kullanıcı özellikleri (işlem kaynakları, depolama kaynakları ve yerel ağ kaynakları yönetimi)
- Sanal dağıtılmış anahtar desteği;
- Ağ güvenliğinin sağlanmasına yönelik çözümlerle entegrasyon;
- Çeşitli bulut altyapıları arasında veri alışverişi için korumalı ağ devresini oluşturma imkânı (Aubakirov, 2016).

2.3.2. Entegre Kamu Hizmetleri İçin Bulut Çözümleri

C-devlet için temel gereksinimler, ilkeler ve amaçlar; e-devlettekilerle bir çok açıdan benzerdir. Ancak, bulut bilişim ve ilgili diğer yeni teknolojiler, özellikle Web 2.0, vatandaşların e-katılımı için etkin araçlar sağlar ve bu durum, çok daha açık ve entegre bir kamu hizmet sunumuna olanak tanır. Bu yeni teknolojilerin e-devlet hizmetleri sunumunda kullanımı, hem kamu kuruluşları ve hem de vatandaş açısından önemli avantajlar sağlar. Bu avantajları şu şekilde sıralayabiliriz:

Kamu kuruluşları için;

- Daha iyi iş süreci yönetimi,
- Maliyet ve zaman tasarrufu,
- Daha doğru ve zamanında bilgi edinme,

- Otomasyon ve süreç iyileştirme,
- Hizmetlerin kolay bakımı ve güncellemesi,
- Diğer birimlerle işbirliği,

Vatandaşlar için;

- Kamu kuruluşlarının e-hizmetlerine kolay erişim,
- Online işlem olanağı, örneğin fatura ödeme,
- Bilgi güvenilirliği ve 7x24 erişilebilirliği,
- Daha doğru ve zamanında bilgi,
- E-katılım için fırsatlar, e-oylama gibi,
- Görüşlerini dile getirme ve kamusal kararları etkileme fırsatları (Mahmood, 2015).

Bulut bilişim ve bulutla ilgili teknolojilerin c-devlet ve e-hizmetlerinin sunumu hususunda ortaya çıkardığı çözümlerin önemlilerine aşağıda yer verilmektedir.

Yazılım Geliştirme Altyapısı için IaaS ve PaaS Servis Modelleri

Kamu kurumları ihtiyaçları olan uygulama yazılımlarını, kendi personeli veya hizmet satın alma yoluyla geliştirebilmek amacıyla, yazılım geliştirme ortamı sunan bilgi işlem altyapılarına gereksinim duyarlar. Bu sebeple, gerek bu altyapılara hiç sahip olmayan ve gerekse de geliştirecekleri spesifik uygulamalar ve bunların test edilebilmesi daha fazla kaynağa ihtiyaç duyan kuruluşlar, Servis olarak Platform (PaaS) ve bu servis modelinin bina edileceği Servis olarak Altyapı (IaaS) hizmetlerini, özel veya eğer varsa kamu bulut sağlayıcılarından temin edebilirler.

PaaS ve IaaS servis modellerini kiralamak, özellikle kısa süreli kullanım için, altyapı yatırımı yapmaktan çok daha ucuzdur. Yine kullandığın kadar öde prensibiyle, atıl kalacak ve kullanılmayacak ölçüde kaynak tedarik edilmeyeceğinden, verimlilik üst düzeydedir. Bakım, güncelleme, arıza, fiziksel kaynak temini ve işletme sorumluluğu genel olarak sağlayıcıya aittir. Özellikle IaaS türünde, sanallaştırılmış kaynakların aşağı

ve yukarı ölçeklendirmesi, gerçek zamanlı ve isteğe bağlı bir şekilde ve gerektiğinde bir operatör müdahalesi yapılabilmektedir. Bütün bu avantaj ve getiriler, günümüzde hemen her kamu kuruluşu tarafından geliştirilen veya temin edilen uygulama yazılımları için, kamu bulutları oluşturulması gerekliliğini güçlü bir şekilde ortaya koymaktadır. Tesis edilecek kamu bulutlarında, benzer uygulamalar için uygulama şablonlarının veya bilişim kaynağı kullanım önerilerinin yer alacağı katalog hizmetleri de kamu kuruluşlarına zaman ve maliyet avantajı sağlayacaktır.

Mevcut Uygulamalar ve E-Hizmetler için SaaS Servis Modeli

Kamu kurulularının vatandaş odaklı geliştirdikleri uygulamalar ve e-hizmetler, işletmeye hazır olduğunda, Servis olarak Yazılım (SaaS) servis modeliyle, kamu veya özel sektör bulut sağlayıcıları tarafından barındırılabilir. Yine burada ilgili kamu kuruluşunun sahip olmadığı herhangi bir özel yazılım ihtiyacı (öreğin veritabanı, işletim sistemi, güvenlik ve yönetim yazılımları), ilgili bulut sağlayıcısı tarafından karşılanabilir. Kamu kuruluşu ilgili uygulamanın kullanımının kontrolüyle ilgili tam yetkiye sahip olurken; bilişim kaynağı kullanım ücretlerini, kullandığın kadar öde prensibiyle ödeyebilecektir. Bakım ve yönetim kontrolü ise bulut sağlayıcısının sorumluluğunda olacaktır. Bulut ortamındaki herhangi bir SaaS, zaman ve platform bağımsız olarak kullanılabilecek ve uygulamanın güvenilirlik ve erişilebilirliği; taraflar arasında düzenlenen hizmet seviye anlaşması (SLA) aracılığıyla bulut sağlayıcısı tarafından garanti edilebilecektir. Yine burada farklı kuruluşların sunacakları yazılımları e-devlet gibi tek çatı altında toplamaları, vatandaşların standartlara dayalı, kaliteli, güvenli ve kolay erişilebilir hizmet almaları açısından önemlidir. Birbirine veri servis eden veya birbiriyle entegre çalışan farklı kurumların spesifik uygulamaları düşünüldüğünde, herhangi bir uygulamada altyapı nedeniyle meydana gelen hizmet aksamasının diğer hizmetlerin de aksamasına neden olması ihtimali, kamu e-hizmetlerinin kamu bulutları gibi ortak altyapılardan sunulmasının gerekliliğini ortaya koymaktadır.

Günümüzde merkez ve taşrada hemen her kamu kuruluşunun, uygulamalarını ve verilerini depolayabilmesi için kendi depolama alanı ve depolama aygıtları mevcuttur. Bu durum ülke genelinde irili ufaklı binlerce veri merkezinin oluşmasına ve bu veri merkezleri için toplamda ciddi işletme ve bakım maliyetleriyle karşı karşıya kalınmasına sebep olmaktadır. Ayrıca birçok durumda tutulan veriler veya sunulan servisler mükerrer olabilmekte ve bu da ciddi bir bilişim kaynağı israfı oluşturmaktadır. Yine kamuda sunulan birçok servis, farklı altyapılarda bulunduğu için farklı güvenlik protokollerine ve farklı destek yazılımlarına (veritabanı, işletim sistemi vb.) sahiptir. Bu durum bu servislerin birbiriyle entegre edilmesi gereken durumlarda, ciddi uyumsuzluklara yol açabilmektedir ve farklı kuruluşlar arasında birlikte çalışılabilirliği ve koordinasyonu tehdit etmektedir. Bu sebeple, bulut ortamı uygulamaları ve verileri barındırmak için en ideal yöntemdir. Bulutun çok kiracılı ve sanallaştırılmış ortamı, performansı üzerinde herhangi bir olumsuz etki yaratmadan, birçok tüketicinin aynı uygulama veya veriye erişebilmesini ve barındırdığı farklı uygulamaların birbirleriyle entegre bir şekilde çalışabilmesini sağlar. Yine güvenlik, gizlilik ve veri yedekleme sağlayıcının sorumluluğunda olduğundan, ihtiyaçlar dâhilinde imzalanacak detaylı hizmet seviye anlaşmalarıyla kamu kurumlarının bu konuda eli güçlendirilebilecektir. Önceki örneklerde olduğu gibi kamusal uygulamaların barındırılması ve verilerin depolanması işlerinin, kamu entegre veri merkezleri gibi ortak altyapılar tarafından sağlanması hususu çok ciddi iş ve maliyet tasarrufları sağlayacaktır.

Kamu Hizmetleri için Hibrit Bulut Mimarisi

Veri mahremiyeti ve güvenliği konusunda kamu kuruluşları tarafından yaşanan endişeler, kısa vadede bütün servislerin açık bulut mimarisi üzerinden sağlanmasını imkânsız kılmaktadır. Bu sebeple kamu kuruluşlarına, birbirlerine ve vatandaşlara servis ettikleri uygulamaları için, aktarılan veya tutulan verilerin gizlilik seviyelerinin dikkate alınacağı hibrit bulut ortamları geliştirmeleri tavsiye edilmektedir. Kurumlar böylece gizlilik derecesi yüksek, kişiye özel veya kendi iç faaliyetleriyle ilgili verileri özel bulut tarafında, gizlilik seviyesi göreceli olarak daha düşük, kamu yararı açısından servis edilmesi gereken verilerini açık bulut tarafında tutabilecektir. Burada açık bulut tarafı,

hem özel hem de kamu bulut sağlayıcıları tarafından sağlanabilecektir. Ancak özel bulut tarafının, özel sektörde faaliyet gösteren bulut sağlayıcılarından temini ciddi riskler içermektedir. Bu sebeple kamu kuruluşlarının, kritik veri ve uygulamaları için ya kendi özel bulutlarını geliştirmeleri veya güvenli bir kamu bulutu hizmetinden faydalanmaları gerekecektir. Kendi özel bulutunu kurma konusunda yeterliliğe sahip olmayan veya tercih etmeyen kamu kuruluşlarına, özel bulut hizmeti sağlayacak bir kamu idaresi oluşturulması, sorunun çözümüne katkı sağlayabilecektir. İlgili kamu idaresi, kamu kuruluşlarının özel bulutlarının tüm sorumluluğuna sahip bir şekilde, yine bu kuruluşların harici açık bulutlarda barındırılan veri ve uygulamalarıyla özel bulutta barındırılan veri ve uygulamaları arasındaki entegrasyonu sağlayabilecektir.

Yazılım Geliştirme ve Uygulama Entegrasyonu için Servis Odaklı Mimari (SOA)

Kamu kuruluşlarının e-hizmetleri, küçük bağımsız web hizmetleri veya diğer servisler ile bağlantılı büyük yazılım uygulamaları olabilir. Bu sebeple ileride farklı uygulamalar ile haberleşemesi, birlikte çalışabilmesi veya birleşmesi olası uygulamaların; Servis Odaklı Mimari (SOA) tasarım felsefesi çerçevesinde geliştirilmesi uygun olacaktır. Bu felsefede geliştirilen her hizmet, son derece uyumlu ve tam fonksiyonel bir birimdir. Her birimin yedekleme, çoğaltılma ve diğer birimlerle entegrasyon ile ilgili güçlü özellikleri, uygulama ve hizmetlerin güncellenmesi ve bakımı ile ilgili ciddi avantajlar sağlamaktadır. SOA tasarım felsefesine sahip bulut ortamındaki bir uygulamada, yapılan güncelleştirme nedeniyle hizmet kesintisi yaşanmaz veya kısa süreli olur. Yine bir uygulama yazılımında bir hata gelişmesi durumunda; yedeklilik, çoğaltma ve yük devretme gibi özellikleri servisin ayakta kalmasını sağlar. Bu durum, bulut ortamının çok kiracılı doğası gereği, çoğaltılması ihtimali göz önünde bulundurularak, hizmetlerin ve uygulamaların sanallaştırılmış bir şekilde tasarlanmış olması sayesindedir.

Vatandaşın E-Katılımı için Web 2.0 ve Sosyal Medya

Web 2.0 ve sosyal medya teknolojileri, e-devlet felsefesinden c-devlete geçişte yardımcı rol oynayan çekirdek teknolojilerdir. Bu teknolojiler yeterli düzeyde bilişim kaynağı altyapısı üzerinde serbestçe kullanılabilir ve vatandaşların görüş ve önerilerini ifade ederek kamusal karar ve tercihlerde belirleyici olmasında rol oynayabilirler. Örneğin vatandaşların ulaşım için kullanacakları belediye otobüslerini veya deniz otobüslerini birkaç alternatif arasından seçebilmeleri bunun bir örneğidir (e-oylama). Başarılı bir c-devlet için, kamu kuruluşlarının sundukları politika ve hizmetlerle ilgili vatandaşların duygu ve düşüncelerini not etmeleri, hizmetlerin sürekliliği açısından önemlidir. Bulut gibi teknolojiler aracılığıyla toplanan verileri analiz etmek ve buna göre cevap vermek zorundadırlar. Bu teknolojiler aracılığıyla toplanan ham veriler, başarılı bir c-devlet için, uygun veri analitiği uygulamaları kullanılarak yapılandırılmalı ve sonuçlar karar vermede kullanılmalıdır. Elde edilen veriler, kamu kuruluşlarının yöneticilerine, sunulan hizmet ve fonksiyonların vatandaş odaklı olup olmadığı konusunda geri bildirim sağlayabilirler.

Kamu Hizmetleri için Kamu Bulutları

Kamu hizmetlerini yerine getirmek amacıyla çok sayıda merkezi ve yerel idareden oluşan, milyonlarca çalışanı olan bir devlet yapılanması, büyük ve karmaşık bir organizasyona benzetilebilir. Kamu idarelerinin yöneticileri değişse bile, bu organizasyon işleyişini devam ettirmelidir. Bilgi ve iletişim teknolojileri ve bu teknolojilerin en güncellerinden olan bulut bilişim hizmet modeli, bu organizasyonel yapıyı daha verimli yönetme ve vatandaşlara daha etkin hizmetler sunma konularında ciddi katkılar sağlar. Kamu kuruluşlarının yukarıda belirtilen servis modellerini farklı sağlayıcılardan temin etmeleri veya kendi özel bulutlarını kurmaları yerine, devletin kendi kamu bulut veya bulutlarını geliştirmesi ve bağlı kuruluşlarına sunması yukarıda da değinildiği üzere; etkinlik, verimlilik, uyumluluk, veri mahremiyeti, esneklik, ölçeklendirilebilirlik, güvenlik ve güvenilirlik gibi birçok konuda ciddi avantajlar sağlayacaktır.

Kamu bulutunun kurulması, işletilmesi, bakımı ve kullanım ile ilgili standartların belirlenmesi amacıyla ayrı bir kamu kuruluşunun ihdas edilmesi veya mevcut bir kamu kuruluşunun görevlendirilmesi; işin tek elden profesyonel bir yaklaşımla yönetilebilmesi açısından önemlidir. Kamu bulutu kurulması konusunda kamu kuruluşlarının uzmanlığı yetersizse, harici bir üçüncü şahıs başlangıçta kamu bulutunu kurmak için görevlendirilebilir. İngiltere, Japonya, Avustralya, Güney Kore, Fransa, Almanya ve daha birçok gelişmiş ülke, halihazırda kendi kamu bulutlarını geliştirmiş ve etkili c-devlet hizmetlerinin sunumunda başarı sağlamışlardır.

2.4. Kamu Bulutu İşletme Modelleri

Entegre kamu hizmetleri için tek bir kamu bulutu veya farklı alanlar için özelleşmiş kamu bulutlarının kurulmasının gerekliliğine ve farklı ülkelerin kamu bulutları tesis etme hususunda attığı adımlar ve geliştirdiği stratejilere önceki bölümlerde değinilmişti. Bu bölümde ise kamu bulutlarının kurulması ve işletilmesi ile ilgili dünya genelinde kullanılan modellere kısaca değinilecektir.

Dünya ülkelerinin kamu bulutu geliştirme çabaları göz önünde bulundurulduğunda, bir çok kamu kuruluşunun ve özellikle de yerel yönetimlerin, kendi özel bulutlarını kurma yönünde strateji belirledikleri ve bu konuda çalışmalara başladıkları anlaşılmaktadır. Ancak her kuruluşun kendi bulutunu kurma isteğinin piyasadaki talebi ve dolayısıyla birim maliyetleri artırabileceği beklentisi, bir çok kamu kuruluşunun özel bulutlarını kurma ve işletme konularında yeterli ödeneğe ve uzman personele sahip olmaması ve en önemlisi kurulacak bulutlar arasında ortaya çıkabilecek teknik ve yasal (ver gizliliği, veri güvenliği vb.) uyumsuzlukların bu kuruluşların birlikte çalışabilirliğini negatif yönde etkileme olasılığı; ülkeleri bir bütün olarak bulut stratejileri belirlemeye ve bu yönde bulut işletme modelleri benimsemeye sevk etmiştir. Bu doğrultuda düya genelinde üç farklı işletme modeli ön plana çıkmaktadır. Bunlar belli bir ajans/kurum liderliğinde bulut, kamu BİT sağlayıcılarının sağladığı bulut ve bulut aracısı (broker) modelleridir.

Ajans/Kurum Liderliğinde Bulut: Bu model, kamu kuruluşlarına çeşitli bulut hizmetlerinin sorunsuz bir şekilde sağlanmasında çekirdek ve merkezi bir rol oynamak üzere özel bir ajans ya da kamu kurumunun görevlendirilmesidir. Bu kurum, kamu kuruluşlarınca ihtiyaç duyulan merkezi tedarik, izleme, yönetim politikalarını belirlemek ve uygulanmaktan sorumludur. Kamu kuruluşlarının ülke genelinde birden çok yerde, devlet tarafından veya deneyimli bir üçüncü taraf kuruluş tarafından yönetilen kendi özel bulutları olabilir. Yine ajans/kurum, bu özel bulutların özellikle verinin gizliliği, güvenliği, kontrolü ve kaybı ile ilgili ortak mevzuatın hazırlanması ve uygulanması ile ilgili gerekli çalışmaları yapabilecektir. Ayrıca bulutların teknik altyapılarının birbiriyle uyumlu çalışabilmesine yönelik gerekli tedbirleri alabilecektir. Yine bu modelde, ajans/kurum tarafından bir veya daha fazla bulut servis sağlayıcısından, sadece ülkeye özel bulutlar kurmaları ve yönetmeleri istenebilir. Burada Afet Kurtarma (DR) bulutları, kamuda yüksek kullanılabilirlik ve veri kurtarmayı garanti etmek için çok önemlidir. Kamu arşivlerinin sağlıklı şekilde barındırılması ve gerektiğinde ihtiyaç duyan kurumlara servis edilmesi ihtiyacı, bu çeşit bir bulut işletme modeli kullanılmasının önemli bir etmenidir.

Birçok ülkede bu görev İçişleri Bakanlığı (örneğin, Polonya, Suudi Arabistan ve Çek Cumhuriyeti'nde) veya Maliye Bakanlığı (örneğin İsrail) tarafından yürütülür. Diğer ülkelerde ise, daha küçük bir ajans/kurum buluta aktarım için devletin çabalarına öncülük etmektedir (Cisco, 2013).

Bu işletme modeline bir örnek Fransa'daki, DILA (Hukuk ve İdari Bilgiler Genel Müdürlüğü)'dır. DILA kanunlara, vatandaş hakları ve görevleri ile kamu hizmetlerinden faydalanmak için gereken bilgilere vatandaşların erişiminin sağlanmasından sorumludur. DILA şu anda kendi operasyonları için kağıt tabanlı süreçlerden, bir Servis olarak Altyapı(IaaS) çözümüne geçmiştir. Aynı zamanda diğer kurumlara bulut hizmetleri sağlamaktadır.

DILA 2012 yılında Accenture firmasıyla kamu faaliyetleri için özelleştirilmiş bulut hizmetleri sağlayan bir kamu bulutu kurulması konusunda sözleşme imzalamıştır.

Kurum, bir kamu bulutu oluşturarak, Fransız vatandaşları ve kamu görevlileri için hizmetlerini standardize etmeyi amaçlamıştır. Ayrıca, daha esnek bir BT altyapısı inşa ederek, ülke genelinde Fransız vatandaşlarına sunulan kamu hizmetlerinin erişim, kullanılabilirlik ve performansını artırmayı hedeflemiştir.Tüm kamusal bilgiler ülkenin bu ilk kamu bulutunda saklanmakta olup, vatandaşların ihtiyaçlarını karşılamak amacıyla, bulutun mimarisinin maliyet kontrolü, çeviklik ve reaktivite açısından tüm faydalarından yararlanılması mümkün olabilmektedir (Zacks Equity Research, 2012).

Ülkemizde Kamu Entegre Veri Merkezi'nin kurulması ve e-devlet platformunun sağlanması ile ilgili T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı sorumlu kuruluştur. Bu işle ilgili diğer kuruluşlarsa Başbakanlık, Kalkınma Bakanlığı, TÜBİTAK ve TÜRKSAT olarak belirlenmiştir.

Kamu BİT Sağlayıcısı: Devletlerin vatandaşlarına karşı bilişim hizmetleriyle ilgili yükümlülüklerinin her türlüsünden sorumlu olmak üzere kurulmuş, bir BİT danışmanlık, çözüm ve servis sağlayıcısı atamasıdır. Kurum/ajans liderliğindeki modelin siyasi karar ile geliştirilerek bağımsız bir teşekkül olarak bir BİT kuruluşunun ayrı bir birim haline getirilip, tamamına ayrıldığı kurumun sahip olduğu bir modeldir. Bu modele BRZ, Avusturya; Statens-IT, Danimarka; SITA, Güney Afrika örnek olarak verilebilir. BRZ ve Statens-IT'nin her ikisi de, ayrı bir birim haline gelmeden önce ilgili ülkelerin Maliye Bakanlıkları altındaki BT departmanlarıydı. Diğer ülkelerde, kamunun paylaşılan BT hizmetleri için ayrı bir birim kuran idare İçişleri Bakanlığı'dır.

Örnek olarak verilen, Bundesrechenzentrum GmbH (BRZ) adındaki Avusturya Federal Bilgi İşlem Merkezi, yüzde yüzüne Avusturya devletinin sahip olduğu ve Avusturya Maliye Bakanlığı tarafından kurulan bir limited şirkettir. BRZ'nin mevcut altyapısı yakın zamana kadar sorunsuz bir şekilde kamu kuruluşlarına hizmet etmiş olup, Adalet Bakanlığı gibi bazı müşteriler için fiziksel olarak ayrı trafik ihtiyacını karşılarken, uygulamalar için daha fazla bant genişliği sağlamak için ek kaynağa ihtiyaç duymuştur. Bu sebeple hizmetlerinin kullanılabilirliğini, hızını ve erişilebilirliğini artırmak amacıyla mimarisini yeniden tasarlamaya karar vermiştir. Kurulan yeni

mimariyle uygulamalar artık çok daha hizmet etkin olup, uygulamaların koştuğu birçok sunucu, çekirdekte 10 Gbps ve erişim ağında en az 2 Gbps hızlardan yararlanabilecek şekilde geliştirilmiştir (Cisco, 2013).

Bulut Aracısı (Broker)/Bulut Entegratörü: Belirli uygulama ve hizmetler için sadece özel bulutlar değil, aynı zamanda açık bulutlar da çok kritiktir. Bu sebeple, kamu kurumları ile bulut servis sağlayıcı arasındaki boşlukları doldurmak ve kesintisiz senkronizasyona yardımcı olmak için, sınıfının en iyisi olan bir servis sağlayıcı seçiminde, bir aracı kuruluş atamak kullanışlı olabilmektedir. NIST rol tanımına göre bir bulut aracısı, bulut hizmetlerinin kullanımını, performansını ve dağıtımını yöneten ve bulut sağlayıcıları ve bulut tüketicileri arasındaki ilişkileri müzakere eden bir kuruluştur. Bulut aracıları, çoklu bulut hizmetlerinin yönetimini kolaylaştırmaya yönelik yöntemler sağlayabilirler. Bir bulut aracısı kurumlara, birden fazla bulut sağlayıcısı arasında birlikte çalışabilirlik sorunlarına odaklanan; işletim ve ilişki destek hizmetleri (fatura ve sözleşme aracılığı, hizmet seçimi ve hizmetleri bir araya toplama gibi işletim desteği) ile birlikte teknik destek hizmetleri (servis toplama, hizmet seçimi, teknik aracılık) sunar (Warren, 2015).

Bulut aracısı sayesinde bakanlıklar ve kuruluşlar açık bulut servislerini seçici olarak kullanabilecek olup, böylece ana misyonlarına odaklanabileceklerdir. Bulut aracısı, ABD'deki Apps.gov gibi klasik bir merkezi satın alma modeli veya hizmetler için entegre bir self-servis portalı olarak temin edilebilir.

Bir bulut aracısı, bulut müşterileri ile hizmeti sağlayan bulut sağlayıcıları arasında bir arabulucu olarak hareket eder. Aracı müşterilere bir dizi hizmetler sağlar ve müşterilerin yönetim sürecini basitleştirir. Ayrıca anlaşmaları (hizmet seviyesi anlaşması ve işletme seviyesi anlaşması) yönetir, ihtiyaç duyulan hizmetleri toplar, bir fiyatlandırma arabuluculuk modeli sunar ve farklı fiyatlandırma modelleri arasında karşılaştırma yapma olanağı sağlar. Aracı ayrıca, müşterinin misyonu olan hedeflerine odaklanmasını sağlamak için, etkileşimin finansal ve operasyonel yönlerini yönetir.

Bir bulut aracısı ayrıca kuruluşlara, bir ya da daha fazla sağlayıcı tarafından temin edilen işlem veya çözümleri sağlar ve bunları yönetir. Yine müşteri yönetimine, örneğin yönetimi kolaylaştırma, müzakere, risk transferi, özel araçları çalıştırma ve birleşik satın alma gücü gibi bileşenlerle destek sağlar. Dengeli bir bulut kaynak portföyü sunarak, bazı durumlarda risk aktarımı yapar ve alıcının daha kurumsal bilgi ve uzmanlıktan faydalanmasına izin verir. Bu durum, yatırımcı için finansal işlemi basitleştirirerek, finansal araçların yatırımcı ve birden fazla teklif sahibi arasında müzakere edilmesine ortam hazırlar.

Emtia piyasalarındaki şirketlerin bir dizi kaynak gereksinimini elde etmesinin sağlandığı özel sektörde olduğu gibi, kamuda da ihtiyaca uygun, nitelikli bulut hizmeti sağlayıcılarının avantajlı tekliflerinden yararlanan bir takas ya da aracı modeliyle, bilgisayar kaynaklarından kâr elde edilebilir. Uzun vadeli sonuçları ve taahhütleri olan sistemleri ve beraberindeki maliyetleri edinmenin aksine (veri merkezi vb alanı, idari personel, lisans, güncellemeler) aracı veya takas modeli, ülkelerin ulusal BT harcamalarının bazılarını, uzun vadeli satıcı bağımlılığı olmayan bir tüketim veya kullanım tabanlı modele taşımalarına izin verir.

Kısacası, kamu BT tedarik pazarı, bulut teknolojileri ve kavramları ile bir kesişim noktasına ulaşmış olup, bu durum bulut aracısı kavramını ortaya çıkararak, bir aracı modelinin uygulanmasından yararlanma fırsatı yaratmıştır. Bu modelde en basit etkileşim, tüketici ve aracı arasındaki doğrudan etkileşimdir ve sözleşmeler, SLA ve diğer anlaşmalar doğrudan yönetilir (Rhody, 2013).

İşletme veya teknik amaçlı bir bulut aracısı kullanmanın faydaları şunlardır:

- Bulutların birlikte çalışabilirliği - Birkaç bulut teklifi arasında entegrasyon,
- Bulut taşınabilirliği - Farklı bulut sağlayıcıları arasında uygulama taşınması,
- Bir bulut sağlayıcıya bağımlılığı azaltarak iş sürekliliğini artırması,

- Çoklu bulut sağlayıcısının katılımıyla Hizmet Seviye Anlaşmalarını sayısını artırması,

- Maliyet tasarrufları - Çoğu IaaS bulut örneği, çok sayıda hizmet satın almış olanlara önemli indirimler sunarlar. Toplam talep hacmi nedeniyle, bulut aracısı kolayca indirimler için hak kazanabilir ve bu durum tüm kullanıcılarına verilen hizmet maliyetini düşürür (Kress, 2015).

2.5. E-Devlet Hizmet ve Uygulamalarının Buluta Aktarılması

2000'li yılların başından bu yana, dünya genelinde kamu kurum ve kuruluşları vatandaşlarına daha şeffaf, hızlı, etkin ve her yerden ulaşılabilir hizmetler sunmak; personel, işyeri ve kırtasiye giderlerini minimize etmek için e-devlet hizmet ve uygulamaları geliştirme yarışına girmişlerdir.

Bilgi teknolojisi tabanlı servisler sağlayan elektronik devlet (e-devlet) üzerinden sunulan kamu hizmetlerinin kapsamı ve kalitesi şu anda sistematik kıyaslama çalışmalarının odak noktasındadır. Düzenli olarak Avrupa Komisyonu tarafından yayımlanan raporlar üreten Avrupa E-Devlet Kıyaslama şeması buna örnek olarak gösterilebilir (Tinholt, 2014).

E-devlet kavramının potansiyel ekonomik ve sosyal faydaları belirgin ve yaygın olarak kabul edilirken, her bir e-devlet hizmetinin uygulanmasında; verimlilik kazanımları, maliyet düşürme, proses optimizasyonu ve diğer iyileştirmeler için hala epey olanak vardır. Bu durum, politik ve teknik karar vericilerin, yeni servisler tasarlarken, teknik ve teknik olmayan çok sayıda faktörü bir arada dikkate almasını gerektirir.

Öte yandan, Bilgi teknolojisi (BT) personeli üzerinde daha az kaynakla daha fazla ve daha iyi faaliyetler gerçekleştirme baskısı artmaktadır. Bu baskı BT personelini yeni teknolojileri benimseme ve işletmeye sevk etmektedir. Bulut bilişim teknolojileri de

bu sebeple, kamu kuruluşları tarafından sunulan e-devlet hizmetlerinin işletilmesinde hızla geleneksel istemci-sunucu mimarisinin yerini almaktadır.

Bulut bilişim e-devlet hizmetlerinin; servis esnekliği (tepe ve dip talepleri karşılama yeteneği), kaynak maliyetlerinin optimizasyonu, ölçeklendirilebilirlik, büyük veri boyutları için kapasite sağlama ve vatandaşlar için internet tabanlı genelleştirilmiş bir erişim modeli sunma gibi temel gereksinimlerini tatmin edici şekilde karşılamaktadır. Bu nedenle, e-devlet platformlarında hızla bulut ve ilgili teknolojilere geçilmektedir. Ayrıca ülkeler, bu hizmetlerin kullanıcı odaklı ve kullanıcı dostu hale getirilmesinin öneminin farkındadırlar. Ancak, hizmetlerin kısa sürede nasıl hazır hale getirileceği ve bu konuda sürekli yeni teknolojik iyileştirmelerin ortaya konulması konularında endişeleri vardır. Ayrıca bazı durumlarda güvenlik ve gizlilik endişeleri, e-devlet hizmetlerinin bulut bilişime aktarılmasının sadece özel bulutlar ile sınırlı kalmasına sebep olsa da, açık ve hibrit bulutların da kullanıldığı birçok uygulama mevcuttur.

Bu endişelere ek olarak, mevcut hizmet ve uygulamalar, gelişen bilgi teknolojilerinin getirdiği kabiliyetlere sahip ve bu bilgi teknolojisi mimarilerine uyumlu olmadıklarından; yeni BİT mimarilerine aktarılmaları ve yeni geliştirilen hizmet ve uygulamalarla entegre edilmeleri konularında zorluklar yaşanmaktadır. Geleneksel istemci-sunucu mimarisine uyumlu şekilde geliştirilmiş bir uygulamanın, bulut bilişim altyapısı üzerine aktarılması için, genellikle büyük bir bölümünün tekrar yazılması gerekmektedir. Dağıtık mimarilere uygun şekilde geliştirilmiş uygulamaların aktarımı ise daha kolaydır ve bazı uygulamalar ufak bazı düzenlemelerle bulut bilişim altyapısına uyumlu hale getirilebilmektedir.

Kurumun BT hizmetlerinin bulut bilişime aktarılması sırasında bir şey yanlış giderse, mevcut sistemlere dönmek kolay değildir. Ayrıca, geleneksel e-devlet hizmetlerinin bulut bilişime aktarılması uzun ve zor bir işlem olabilir (Gongolidis, 2014).

Bu sebeple, kurumların bulut bilişimin kendileri için en iyi seçim olduğundan ve aktarımın en uygun şekilde yapıldığından emin olabilmeleri ve yaşanabilecek sorunların üstesinden gelebilmeleri için; aktarım sürecini dikkatlice planlanmaları ve uygulamaları gerekmektedir. Bu bölümde adım adım e-devlet hizmet, uygulama, veri ve altyapılarının buluta aktarım sürecine yer verilecektir. Bulut bilişime aktarım sürecinde gerek müşteri konumundaki kamu kurum ve kuruluşlarının ve gerekse de satıcı pozisyonundaki servis sağlayıcının ayrı ayrı görev ve sorumlulukları vardır. Burada özellikle, kurumların bu süreçte yapmaları gerekenler açıklanacak ve müteakiben sağlayıcıların sorumluluklarına kısaca değinilecektir. Bu süreçte kuruluşların hizmetlerini, uygulamalarını, veri ve altyapılarını buluta aktarabilmek için aşağıda adımlarda belirtilen faaliyetleri gerçekleştirmesi gerekmektedir.

2.5.1. Strateji Tanımlama

Bu süreç kuruluşun BT departmanının, kuruluş yönetimi ile işbirliği içinde, hizmetlerini bulut bilişime aktarmaya başlamadan önce yürüttüğü bir ön süreçtir. Kuruluşun BT yöneticileri ve karar vericilerin, bulut bilişimin benimsenip benimsenmeyeceği ile ilgili kesin bir karara varmaları gerekmektedir. Bu işlemde, kuruluş öncelikle bulut bilişim hakkında bilgi toplar ve bulut yaklaşımının esaslarını anlamaya ve kuruluşun bulut bilişim mimarisine geçişinin nedenlerini açıklamaya çalışır. Bu noktada kuruluşların hizmetlerine bulutun katacağı gerçek değeri dikkate alması, sadece yeni trendleri takip etmek yerine, ihtiyaçlarını daha etkin bir şekilde sağlamak amacıyla bulut bilişime geçiş yapması gerekmektedir. Bulut tabanlı hizmet modeli ile kuruluşun yapısal ve işletim modeli arasındaki uyuşma değerlendirilirken, sunulan iş ve hizmetlerle ilgili bilgi toplamak en az teknik ihtiyaçların belirlenmesi kadar önemlidir (Ezzat, 2011).

Yine karar vericiler, bulut bilişimin yaratacağı değişikliklerin kurumsal etkilerini dikkate almalıdırlar. Ayrıca kuruluşun hedeflerini açıkça ortaya koyan ve finansal tedarik yöntemlerinin belirlenmesini içeren aktarım stratejisi geliştirmelidir.

2.5.2. Mevcut Mimariyi Belirleme ve Anlama

Kuruluşun hizmet ve uygulamalarını buluta aktarım kararının nedenlerini ve muhtemel sonuçlarını belirledikten sonra, BT altyapısına ilişkin ayrıntılı bilgi toplamak gereklidir. Böylece, sözkonusu hizmet ve uygulamaların birbirleriyle olan ilişkilerinin hassasiyetle farkına varılabilir ve kuruluşun hangi hizmet birimlerinin buluta aktarılacağına ve hangi birimlerinin mevcut altyapı üzerinde kalacağına karar verilebilir. Birbiriyle entegre çalışan, aralarında veri alış-verişi olan uygulamaları sekteye uğratmamak için; buluta aktarılacak varlıkları doğru tahmin etmek ve kuruluşun şartlarına göre en iyi alternatifi seçmek önemlidir. Bu süreçte BT personeli, karar verici işbirliği ile BT hizmetleri, uygulamalar ve ilgili veriler hakkında ayrıntılı bilgi toplamalıdır (Tusanova, 2012).

Bu bilgiler, uygulama ve hizmetlerle ilgili güvenlik, iletişim, erişim, maliyet, birbirine bağımlılık, değer, kullanılabilirlik, yararlar, gereksinimler ve kullanılan kaynaklar gibi ayrıntıları içerir. Maliyetler ile ilgili bilgiler, kurumun mevcut uygulamaları ile bulut bilişim mimarisinde işletilecek emsallariyle ilgili işletme maliyeti karşılaştırması için temel teşkil edecektir. Burada kurum eğer iç hizmetlerini buluta aktarıyorsa, aktardığı öğelerin her birinin iş kritiklikliğine özel olarak dikkat etmelidir. Temel ve kritik uygulamaların buluta aktarımı özel dikkat gerektirmekte olup; bu sebeple bu uygulamaların hangileri olduğu dikkatlice belirlenmelidir. Sistemin iyi analiz edilebilmesi ve raporlanan sorunların azaltılabilmesi için, kuruluşun yardım masası hizmet sorgu ve cevap kayıtları önemli bir bilgi kaynağı teşkil etmektedir (Khajeh-Hosseini, 2010).

Hizmetler: Hangi uygulamaların buluta aktarılacağı ve hangilerinin mevcut sistemde tutulacağı hakkında en uygun kararı verebilmek adına; buluta aktarımdan sorumlu BT personelinin, kuruluş tarafından sağlanan hizmetlerin tüm ayrıntılarını kavraması gerekir. Sağlanan hizmetlerin kullandığı uygulamalar, veriler ve altyapı hakkında bir liste hazırlanmalıdır. Ayrıca, çeşitli hizmetler arasındaki etkileşimlerin ve birbirleriyle olan veri alış-verişinin tanımlanması gerekmektedir. Mevcut hizmetlerin tedarik ve

sunumuyla ilgili maliyet bilgileri, bulut mimarisindeki emsalleri ile daha sonra karşılaştırma yapılabilmek için gereklidir. Son olarak, BT personelinin erişim düzeyleri ve gerekli güvenlik derecesi gibi güvenlik gereksinimleri de dikkate alınmalıdır.

Uygulamalar: Uygulamalar BT hizmetlerinin ana bileşenlerinden biridir. Bulut bilişim mimarisinde yeni bir uygulama geliştirmek kolay olsa da, mevcut uygulamaların buluta aktarılıp aktarılamayacağı belli değildir. Uygulamalara ilişkin bilgi toplama sürecinde, BT yöneticilerinin uygulamaların ayrıntılı açıklamalarını içeren ve aralarındaki etkileşimleri tarifleyen bir liste hazırlamaları gerekir. Ayrıca, uygulamaların kullandıkları veri ve kaynaklar, sorumlu personel ve teknik ekipmanlar gibi bilgileri toplamaları gerekir. Hizmette olduğu gibi, kurum içi uygulamaların her birinin buluta aktarımından sağlanacak maliyet faydasını tespit etmek için, maliyetlerine ilişkin bilgiler de gereklidir.

Bir uygulamanın buluta aktarımı genellikle üç farklı şekilde yapılabilir. Bunların ilki, bir uygulamanın zaten bulutta mevcut olan başka bir uygulamayla değiştirilmesine dayanır. Burada mevcut uygulamanın verilerinin alınıp bulut uygulamasına aktarılması sağlanır. İkincisi, bulut üzerindeki bir uygulama geliştirme platformunda, mevcut uygulamayla aynı görevi yapacak yeni bir uygulama geliştirmektir. Üçüncü de ise uygulama sadece bulut altyapısındaki bir sunucuya taşınır. Bu yöntem, uygulamalarını değiştirmek zorunda kalmadan buluta aktarmaya imkân tanıdığı için, kuruluşlar için tartışmasız en cazip olanıdır. Burada mevcut altyapıda birbiriyle entegre olan programların bulutta ne şekilde entegre edilebileceği iyi planlanmalıdır. Ayrıca, özellikle açık ve hibrit bulutlar için, sağlayıcı altyapısına aktarılan kuruluş bilgilerinin ileride ne şekilde geri alınabileceğini belirlemek, sağlayıcıya bağımlılığı önlemek için gereklidir.

Uygulamalar genelde sunum, iş mantığı ve veriler adında üç katmandan oluşurlar. Bu katmanların herbiri için farklı araçlar kullanılarak, ayrı ayrı buluta aktarılmaları gerekecektir. Özetle uygulamaların buluta aktarımı sürecinde aşağıda sıralanan konuların çözülmesi gerekir:

- Uygulamaların hangi bölümlerinin buluta aktarılması gerektiğinin tanımlanması,
- Hangi bulut servis modellerinin kullanılması gerektiğinin belirlenmesi,
- Uygulamanın herhangi bir parçasının mevcut sistemde kalmasının gerekip gerekmediğinin belirlenmesi (örneğin güvenlik nedeniyle)
- Bir veya birkaç sağlayıcının kullanılıp kullanılmayacağının belirlenmesi (uyumluluk sorunları ortaya çıkabilecektir),
- Uygulamalarda yapılan değişikliklerin nasıl bir etki yaratacağının değerlendirilmesi,
- Bu yeni mimariye uyum için, uygulamanın ne şekilde yeniden kodlanması gerektiğinin belirlenmesi (Andrikopoulos, 2013).

Veri: Buluta veri aktarımı planlanırken, BT yöneticilerinin odaklanması gereken konulardan biri, veri tanımı oluşturabilmek için; verinin boyutu, biçimi, kaynağı ve farklı veri kümeleri arasındaki ilişki de dâhil olmak üzere tüm ayrıntılarını belirlemektir. Verilerin buluta aktarımı, güvenlik riskini artırır ve kontrol ve yönetimlerinde aksamalara neden olur. Bu sebeple, verilerin buluta aktarım için uygun olup olmadığına karar verebilmek amacıyla; güvenlik ilkeleri tanımlamak, gizlilik ihtiyacı, erişim derecesi ve bilgi önem durumunu değerlendirmek gereklidir. E-devlet hizmetlerinin birçoğu vatandaşların kişisel bilgilerini kullanır. Bu sebeple, ilgili ülke mevzuatında kişisel bilgileri ele alan yasalara ilişkin ortaya çıkabilecek sorunlar öngörülmelidir. Ayrıca, bazı sağlayıcılar ağ veri trafiği için ekstra ücretler talep edebildiklerinden; bulut ile veri alışverişi ihtiyacı, gelen veya giden veri aktarım miktarı veya sağlayıcının altyapısı içindeki veri transferi gibi diğer gizli maliyetlerin varlığının aktarımdan önce değerlendirilmesi gerekmektedir (Martens, 2012).

2.5.3. Buluta Aktarım Planı Hazırlama

Bu adım buluta neyin aktarılacağı ve ne zaman aktarılacağı gibi ayrıntılara karar vermek ve bunları tanımlamak ile ilgili faaliyetleri kapsamaktadır. Bu süreçte, önceki adımlarda mevcut mimari ile ilgili sağlanan bilgiler işlenerek, kullanılmak üzere sonraki

adımlara aktarılırlar. Buluta aktarım planı hazırlanması, kuruluşun bütün aktarım sürecine katılımını ve BT personeli ile kuruluş arasında tam bir uyumu sağlamak için; BT personeli ve kuruluş yönetimi arasında işbirliği ile yürütülmelidir. Çeşitli alt adımlar aşağıda detaylandırılmıştır.

Personel Görevlendirme: Burada amaç buluta aktarım sürecinde, her bir aktarım için hangi personelin sorumlu ve yardımcı olacağını tanımlamaktır. Oluşturulacak proje ekibinde BT personelinin yanında; işletme yönetimi, finans yönetimi ve hukuki destek ile ilgili katkı sağlayabilecek personelin de bulunması gerekmektedir. Ayrıca farklı birimlerin sunduğu uygulamalar için, ilgili birimden söz konusu uygulamanın tüm özelliklerine hâkim personelin bulunması kritiktir.

Görev ve Sorumluluklar: Kuruluşların hizmet ve uygulamalarını buluta aktarmadan önce, sorumluluklarının bilincinde olmaları ve bu sorumluluklara aktarım sırasında uymaları zorunludur. Bu sebeple kuruluş, tüm süreci kimin yöneteceğini, sağlayıcı ile ilişkileri kimin yöneteceğini ve her bir katılımcının sorumluluklarını tanımlamalı; ayrıca sürece kimlerin katkı sağlayabilecek bilgi ve deneyime sahip olduğuna açıkça karar vermelidir.

Nelerin aktarılacağının belirlenmesi: Buluta aktarımdan sorumlu personelin, önceki adım ve süreçlerden edindikleri bilgiler ile sağlayıcıdan gelen gereksinimleri değerlendirerek; kuruluş yönetiminin kararları doğrultusunda, hangi hizmet ve uygulamaların aktarılacağını belirlemesi gerekir.

Güvenlik: BT ve diğer personel buluta aktarılacak hizmetler, uygulamalar ve veriler ile ilgili güvenlik gereksinimlerini tanımlarlar. Uygulama ve hizmetlerin sahibi kuruluş tarafından kontrol edilen geleneksel BT ortamından, bir veya birden fazla sağlayıcıya ve çok sayıda kullanıcıya dayanan bir ortama geçiş, kuruluşların risk ve güvenlik yönetimlerinde önemli değişikliklere yol açacaktır. Güvenlik, gizlilik ve bütünlük bulut bilişim mimarisinin kullanımıyla ortaya çıkan ana konulardan bazılarıdır.

Erişim: Bulut bilişim servislerine erişimin genellikle internet üzerinden yapıldığı dikkate alınarak, erişim kontrolü tanımlanmalıdır. Kuruluşun sunduğu mevcut BT çözümlerinde erişim yetkisi tanımlanması kuruluşun kontrolü altındayken, bulut bilişimde erişim yetkisi tanımlanması direkt olarak kuruluşun sistem yöneticilerinin kontrolünde değildir. Bu sebeple, buluta aktarımdan sorumlu personel, önceki süreçlerde yapılan çalışmalar sonucu toplanan bilgilere dayanarak; her hizmet için erişim yetki ve bilgilerini, buluta aktarılacak uygulamalar ve veriler için tanımlamalıdır.

Bulut türleri: Buluta aktarım süreci benimsenen bulut türüne bağlıdır. Uygun modeli seçerken kuruluşun; uygulamaları için trafik yoğunluğu, güvenlik ve entegrasyon gereksinimlerini değerlendirilmesi gerekmektedir. Bu seçim, sağlayıcı seçimi alt adımında elde edilen bilgiler doğrultusunda yapılır.

Sağlayıcı sayısı: Kuruluş bulut mimarisinde kaç sağlayıcıyla birlikte çalışacağını ve bu sağlayıcıların birlikte çalışabilirliğini; aktarılacak ve mevcut sistemde kalacak hizmet ve uygulamalarını göz önünde bulundurarak tanımlamalıdır. Kuruluş hizmet ve uygulamalarını sağlayıcıya teslim etmeden önce; verilerinin içe ve dışa aktarımı ile ilgili mümkün olduğunca fazla miktarda bilgilendirmeyi sağlayıcıdan talep etmelidir. Çünkü eğer veri ve uygulamalarını, başka sağlayıcıya veya kurum içindeki mevcut sistemine geri taşıması mümkün değilse; bu durum sağlayıcı bağımlılığı veya veri kaybı gibi ciddi sorunlara neden olabilecektir. Ayrıca birlikte çalışabilirlik eksikliği de bir yedek sağlayıcıya olan ihtiyacı tehlikeye atabilir.

Birlikte çalışabilirlik sorunları ancak standartların kullanımı ile aşılabilir. Bu standartların bir örneği Dağıtılmış Yönetim Görev Gücü adlı Açık Sanallaştırma Biçimi (OVF) 'dir. Bu Servis olarak Altyapı (IaaS) sağlayıcıları arasında, sanal makine (VM) birlikte çalışabilirliğini sağlamak için oluşturulan bir standarttır. Yönetim alanında, Açık Bulut Bilişim Arabirimi (OCCI), uzaktan yönetilen bulut altyapıları için protokol ve API özelliklerini belirler. Diğer bir yönetim standardı olan CDMI (Bulut Veri Yönetimi Arabirimi) ise; bulut veri öğelerini oluşturmak, almak, güncellemek ve silmek için kullanılan bir uygulama arayüzü tanımlar (SNIA, 2014).

2.5.4. Sağlayıcı Seçimi

Bulut bilişim hizmet seçiminde başlıca sorunlardan biri de, çok geniş bir yelpazedeki bulut bilişim çözümlerinin bir sağlayıcıyı diğerleriyle karşılaştırmayı zorlaştırmasıdır. Bu süreçte, kuruluşlar ihtiyaçlarına en uygun bulut bilişim çözümünü bulmak için sağlayıcı piyasasında araştırma yapmalıdırlar. Sağlayıcı seçiminde birim fiyat ve bilişim kaynaklarının performansına ek olarak; kullanılabilirlik, güvenlik, müşteriler ile sağlayıcı arasındaki iletişim hatlarının kalitesi, sağlayıcının piyasa itibarı, yasal ve kurumsal faktörler gibi birçok faktör dikkate alınır. Bunun yanı sıra, bir sağlayıcının mevcut müşterilerinin güveni, sağlayıcı seçiminde önemli bir faktördür (Beserra, 2012).

Belirleme: Sağlayıcı seçimi öncelikle potansiyel sağlayıcıların belirlenmesiyle başlar. Bu seçim, kuruluşun önceki adımlarda belirlenen gereksinimlerine uyularak ve aktarım projesinin kuruluşun beklentilerine uygunluğuna karar verilerek yapılır. Bu nedenle kuruluşlar, sağlayıcının sunduğu her hizmetin; yapılandırması için gerekli zaman, güncellemeleri arasında geçen süre, servis kapasitesini azaltmak ve artırmak için gerekli süre ve yedekleme politikaları gibi kriterleri ele almak zorundadırlar.

Her bulut servis modelinin, kendine has artıları ve eksileri vardır. Örneğin Servis olarak Altyapı (IaaS) modelinde, kuruluşların uygulamaları için gerekli bilişim kaynak ihtiyaçları hakkında daha fazla ön bilgiye sahip olmaları gerekirken, sağlayıcıya bağımlılıkları azdır. Servis olarak Platform (PaaS) modelindeyse, geliştirme süresinin belirlenmesi kritik olup; müşterinin sağlayıcıya bağımlılığı çok daha fazladır. Servis olarak Yazılımın (SaaS) yönetimi kolaydır ve kuruluşun sorumlulukları minimum düzeydedir ancak bu model standart uygulamaların kullanımını gerektirir ve bu durum sözleşme sonunda kuruluşun verilerini elde etmesinin daha zor olabileceği anlamına gelir.

Seçim: En uygun potansiyel sağlayıcıları belirledikten sonra, kuruluş bu adaylardan çalışacağı bir veya birkaç tanesini seçmelidir. Bulut hizmeti temin edilecek bu sağlayıcıları seçerken kuruluşun; her sağlayıcının piyasa deneyimini, teknik uzmanlığını,

pazardaki itibarını, kredi imkânlarını, şirket istikrarını ve güven sorununu değerlendirmesi gerekir. Ayrıca, hizmet için iyi bir bilgi kaynağı olarak, gerçek aktarımda kullanılan hizmetlerin ücretsiz denemesi şeklinde ve seçilen sağlayıcıların hizmetlerini kullanan diğer müşterilere sorular sorulması amacıyla canlı bir test ayarlanabilir. Müşterilerin belirlediği sağlayıcıların performanslarının ve maliyetlerinin sistematik olarak karşılaştırması, CloudCmp aracı kullanılarak yapılabilmektedir (Li, 2010).

2.5.5. Analiz ve Test

Aktarım süreci ile ilgili kritik kararlar verildikten sonra, bu adımda, süreçle ilgili tüm bileşenlerin gereksinimlere uygun olup olmadığı analiz ve test edilecektir.

Etki: Bulut bilişim, kuruluşların BT ve iş hizmetlerini sunma metodlarını değiştirir ve ne kadar iyi planlansa da, etkilerinin ne olacağı her zaman açık değildir. Bu sebeple, mümkün mertebe hizmet ve uygulamalarının buluta aktarılmasının, kuruluşa ne gibi etkileri olacağının irdelenmesi gerekmektedir. Yapılacak değişikliklerle kuruluşun hangi hizmet alanlarının etkileneceğini keşfetmek için çalışma yapılmalıdır. Örneğin bulut bilişime geçildiğinde, mevcut bir hizmetin yerine yeni bir ürün veya hizmet oluşturmak veya kiralamak mümkündür. Ancak eğer bu yeni hizmet önemli miktarda işlem gücü gerektiriyorsa ve maliyet etkin değilse eski hizmeti devam ettirmek daha mantıklıdır. Ayrıca bu adımda kuruluşun, sağlayıcının uzun süreli bir hizmet kesintisi ya da iflası sebepleriyle hizmet veremediği durumlarda, ne şekilde etkileneceği de analiz edilmelidir.

Güvenlik: Teknik açıdan bakıldığında, bulut bilişimde karşılaşılan çoğu güvenlik sorunu zaten geleneksel bilişim mimarilerinde de mevcuttur. Burada kuruluş, sağlayıcının güvenlik gereksinimlerini ve şart koşulan operasyonel güvenlik standartlarını karşılayıp karşılamadığını kontrol etmelidir. Ayrıca altyapının yanı sıra, faaliyetlerin ve sonuçların kayıtları (logları) gibi, kuruluşun ele alması gereken başka güvenlik hususları vardır ve bu bilgiler sağlayıcıdan elde edilebilir (Kandukuri, 2009).

Güvenliğe ve yasal gerekliliklere ilişkin, adli bir analiz yapabilmek için kuruluş, bilgilerin ne kadar süre depolandığını kontrol etmelidir. Son olarak kuruluşun, herhangi bir güvenlik ihlali olup olmadığını ve verilerinin bir şekilde riske atılıp atılmadığını bilmesi gerekir. Çünkü yaşanan olayda sağlayıcının yasal sorumluluğu olabilir ancak kuruluş genellikle durumdan en çok etkilenen nihai sorumluluk sahibidir (Guo, 2010).

Sözleşme ve Hizmet Seviye Anlaşması (SLA): Her geçen gün daha fazla kuruluş sağlayıcılara kendi görevlerini devrettiğinden, kuruluşlar ve sağlayıcılar arasında yapılan Hizmet Seviye Anlaşmları (SLA) önemli bir faktör haline gelmektedir. Uygun bir SLA; hizmet süresi, hata ve arıza çözme süresi, performans, tepki süresi, güvenlik önlemleri ve kullanılan terimlerin tanımı gibi öğeleri içermelidir. Sağlayıcı ile SLA imzalandığında, kuruluşun hizmet ve uygulamalarının en kritik özellikleri vurgulanmalıdır ve böylece sağlayıcılar bu konularda daha sıkı tedbirler uygulayabilmelidirler. Kuruluşun, SLA hükümlerini nasıl geçerli kılacağını öğrenmesi ve belirtilen hizmetleri nasıl kontrol edeceğini bilmesi gerekir.

Performans ve hizmet kalitesi üzerine odaklanan SLA'nın aksine sözleşme; maliyet, süre, hazır bulundurulan ve kullanılan kaynaklar gibi faktörler ile sağlanan hizmetleri açıklayan yasal bir belgedir. Sözleşme, feshi halinde meydana gelecekleri şart koymalıdır. Bu doğrultuda, müşteri veri ve uygulamalarının alınması için olası formatlar nelerdir, bunların maliyetleri nedir ve sağlayıcı tarafından ne gibi destekler sağlanmaktadır; sorularının cevapları açıkça belirtilmelidir. Buna ek olarak sağlayıcının, kuruluşun verisinin nasıl silineceğini ve bunun uygun bir şekilde yapıldığına dair ne gibi garantileri olduğunu açıklaması gerekir (Onwudebelu, 2012).

Riskler: Buluta aktarım, süreç içerisinde analiz edilerek hafifletilebilecek bir dizi riski beraberinde getirir. Bu sebeple, buluta aktarım ve seçilen modellere özel riskler hakkında çalışma yapmak gerekmektedir. Genel olarak, hizmetlerin bulut bilişime aktarımına ilişkin dört temel risk alanı tanımlanmıştır. Bunlar kurumsal, teknik, hukuki ve ortak risklerdir. Kurumsal riskler sağlayıcının hizmeti kapatması, sağlayıcı bağımlılığı, hizmet sunumunun eksikliği ve hizmet kesintilerini içerirken, teknik riskler

altyapının yetersizliği, kötü niyetli faaliyetler, veri hasarı ve yazılım açıkları durumlarında ortaya çıkar. Yasal kanıt sağlama yetersizliği, yargı yetkisi ve yazılım lisanslama değişiklikleri hukuki riskler olarak ortaya çıkarken; ortak riskler içerisinde doğal afetler, yedekleme hataları ve veri ifşası yer almaktadır.

Bulut bilişim kullanımında, e-devlet hizmetleri için bazı risklerde bir düşüş görülür. Örneğin, geleneksel mimarilerde vatandaşların e-devlet hizmetlerini benimsemeyip, yazılı ve ıslak imzalı belgeler gibi geleneksel yöntemleri kullanmayı tercih etmesi, büyük miktarda donanımın durması ve atıl kalması gibi bir risk yaratır. Ancak bulut bilişim kaynaklarının kolayca edinilebilmesi ve serbest bırakılabilmesi avantajı sayesinde bu risk ortadan kaybolur.

Personel: Buluta aktarım süreci sonunda kuruluşun hizmet ve uygulamalarının bazılarının sona ermesi ve bazılarının yeniden tasarlanmış şekilde varlığını sürdürmesi, kuruluşun yaşanabilecek personel sorunlarını da göz önüne almasını gerektirir çünkü bulut bilişime aktarım başta BT personeli olmak üzere istihdam sorunlarına neden olur. Bu sebeple, kuruluş artık gerekli olmayan çalışanları ile ne yapacağını planlamalı, örneğin rollerini yeniden tasarlamalı, onları eğiterek yeni beceriler kazanmaya teşvik etmeli ve diğer çalışanlardan bu değişikliklere karşı oluşabilecek tepkilere hazırlıklı olmalıdır (Alkhalil, 2013).

Yasalar: Kuruluşun ister mevcut altyapıda ve isterse de bulutta barındırılsın, uygulamaları ve verilerine ilişkin yasal gerekliliklerin neler olduğuna dair ayrıntılı bir değerlendirme yapması ve bunların bulut bilişim mimarisinde barındırılmasının yasal şartlara uygun olup olmadığını kontrol etmesi gerekir. Farklı lokasyonlarda farklı yargı kuralları olabileceğinden ve bunun bir sonucu olarak, aynı verilere nerede saklandığına bağlı olarak farklı yasalar uygulanabilineceğinden; kuruluşun verisinin konumunu tam olarak bilmesi gerekmektedir.

Bulut bilişim faydalarından biri bilginin soyutlanmasıdır. Bilgi genellikle bakım ve depolama için daha ekonomik olan bir yerde tutulur. Sağlanan teknoloji, fiziksel

konumu hakkında bildirime gerek kalmadan bilgiye erişimi destekler. Bulut bilişimin dinamik yapısının ve bulut hizmet sağlayıcısının verileri nerede depoladığı hakkındaki belirsizliğin bir dezavantajıysa, kuruluşların verilerine uygulanması gereken kanunların geçerli olmadığı lokasyonlarda barındırılmaları ihtimalidir. Örneğin Google, Microsoft ve Amazon gibi bulut sağlayıcı veri merkezleri, Amerika Birleşik Devletleri (ABD) ve Avrupa Birliği (AB) sınırlarında yer almaktadır. Ancak, her iki bölgenin vatandaşları da bilgilerinin gizliliğinin korunması konusunda aynı endişeleri taşıyor olsalar da, ABD tarafından benimsenen yaklaşım AB'den farklıdır. ABD, bazı kişisel bilgileri (örneğin tıbbi veriler gibi) yasal koruma garantisinde, diğer bilgileriyse (örneğin mali konular gibi) gizlenebilir ya da açığa çıkarılabilir olarak değerlendirirken; AB ülkeleri tüm kişisel bilgilerin mahremiyetinin temel bir insan hakkı olup, yasalara göre korunması gerektiğine inanmaktadır.

Sözleşmelerde sağlayıcının buluttaki sorumluluk alanlarının öngörülebilmesini sağlamak için, uygun hukuki danışmanlık almak esastır. Müşteri, veri ve uygulamalarına hangi yasaların uygulanacağı ve bunların kurum içinde mi yoksa bulutta mı tutulacağını belirleme konularında dikkatli olmalıdır.

Avantajlar ve sorunlar: Bulut bilişimin sağladığı birçok faydanın yanında, ortaya çıkardığı bir dizi sorunlar da vardır. Bu adımda kuruluş, geleneksel mimariler ile bulut çözümlerini karşılaştırmak adına, bunların artılarını ve eksilerini tartacak ve sonuçta kuruluş için en uygun olanını seçecektir.

İletişim: Bulut bilişimde kuruluşlar uzak sağlayıcılardan BT hizmetleri sağlar ve internet üzerinden bu hizmetlerden faydalanırlar. Hizmetlerin internet üzerinden sağlanması ve kullanımı, verimlilikte bir artışa yol açar ve her yerden erişimi mümkün kılar. Bunun aksine, sistem içerisindeki iletişim ve özellikle de internet erişimi kolayca bir tıkanıklığa yol açabileceğinden ve başlı başına bir hata noktası haline gelebileceğinden; kuruluş tarafından özel bir ilgiyi hak etmektedir. Kuruluşun, internet yoluyla taşınan veri boyutunu iyi değerlendirmesi ve bu doğrultuda gerekli kapasiteyi, yedekleme hattını, güvenlik, maliyet ve veri şifreleme ihtiyacını belirlemesi gerekir. Bu

çalışmalar bilgi sızması, gecikmeler ve bilgi ve uygulamalara erişim yetersizliği gibi olası sorunları önlemek için gereklidir (Cochran, 2011).

Ayrıca, kuruluşların iletişim hizmetlerinin maliyetlerini bilmesi ve ihtiyaçlarının karşılanmasını sağlamak için, sağlayıcının sunduğu koşulları iyi anlaması gerekir. Bulut bilişimde, e-devlet hizmetleri için veri trafiğinin çoğunun vatandaşlar ve bulut sağlayıcıları arasında olduğu hususu göz önüne alınarak; kamu kurumu ve sağlayıcı arasındaki ile vatandaşlar ve sağlayıcı arasındaki trafik gereksinimlerini iyi belirlenmelidir.

Uygulamalar ve veri: Bulut uygulamalarının üç grubu vardır. İlk grup, kuruluşlar tarafından buluta aktarılmış veya bulutta oluşturulmuş ve Servis olarak Altyapı (IaaS) veya Servis olarak Platform (PaaS) servis modelleri aracılığıyla yaygın olarak kullanılan uygulamaları içerir. Burada kuruluşun; güvenlik, bütünlük, kuruluş bilgilerine kimlerin erişim yetkisi olduğu, güncellemelerin nasıl yapıldığı, yedeklemenin ve yedek kopyalarının nasıl alındığı, uygulamaların içe ve dışa aktarımında ne gibi yöntemler uygulandığı, farklı sağlayıcılar arasında uygulamaların taşınabilme seviyesi ve uygulamaların nasıl test edebileceği konularını analiz etmesi gereklidir.

İkinci grup (Servis olarak Yazılım (SaaS) modeli), sağlayıcının müşterilerine sunduğu uygulamalar ile bu uygulamaları kullanılabilir hale getirmek için kullandığı diğer yazılımlardır. Kuruluşun, bu uygulamaları kendi ihtiyaçlarına göre ayarlamak için, ne tür özelleştirmelerin yapılabileceğini araştırması gerekir. Ayrıca güvenilirliği artırmak için bu uygulamaları kimin geliştirdiğinin, nerede ve kim tarafından test edildiğinin bilinmesi gerekir. Müşterinin ayrıca, bildirimler ve farklı sürümlerle uyumlulukla ilgili sorunlar yaşaması ihtimaline karşı, yazılım yükseltme prosedürünün ayrıntıları hakkında bilgi toplaması gerekir.

Üçüncü grup ise, bulutu yönetmek için sağlayıcı tarafından kullanılan uygulamaları kapsamaktadır. Bu uygulamaların, kimin tarafından geliştirildiğinin ve test

edildiğinin, nasıl izlenebileceklerinin ve müşteri bilgilerinin erişilebilir ve güvenli olup olmadığının kuruluş tarafından bilinmesi gerekmektedir.

Verinin kuruluş tarafından içe ve dışa aktarımı ile ilgili; sağlanan desteğin türü, bilgi transferinde uygulanan standartlar ve bulut veri aktarım maliyetleri ile ilgili bilgiler sağlayıcıdan alınmalıdır. Veri depolama konusunda ise, kuruluşun; veri depolama için kullanılan veri formatları ve standartlarını, verilerin saklandığı yerleri, verilere erişimi düzenleyen mevzuat ile birlikte depolamayı kimin yönettiğini iyi bilmesi gerekmektedir.

2.5.6. Haritalama

Bu adımda, önceki süreçlerde toplanan ve onaylanan tüm bilgilere dayanarak, mevcut bilişim altyapısında bulunan hizmet ve uygulamaların, bulut bilişime aktarılmasına karar verilmeleri durumunda, bulut mimarisindeki emsalleriyle ne ölçüde eşleşeceğini kuruluşların tanımlaması gerekmektedir.

2.5.7. Aktarma ve Yönetim

Bu adım, hizmetin buluta aktarımına ilişkin son süreçtir. Üretim ortamına geçmeden önce, yeni mimariyi test etmek için bir pilot uygulama yüklenir ve bu şekilde yeni sistemin işlevlerinin beklendiği gibi çalışıp çalışmadığını belirlenebilir. Bu pilot uygulama başarı ile gerçekleştirdikten sonra, üretim ortamına bütün mimari (kurum içi ve bulut) aktarılabilecektir. Ancak her şeyin sorunsuz çalıştığından emin olmak için daha fazla test yapmak gereklidir. Bu sayede; sürekli iyileştirmeler yapmak, süreci izlemek, hizmet kalitesini onaylamak ve dolayısıyla SLA'nın ve sözleşme şartlarının yerine getirilip getirilmediğini değerlendirmek ve onaylamak mümkün olacaktır.

2.6. Kamuda Bulut Bilişim Kullanımının Faydaları ve Sorunlar

2.6.1. Kamuda Bulut Bilişim Kullanımının Faydaları

Günümüzde bilişim teknolojilerinin gelişiminin sağladığı avantajlar, özel sektörde olduğu gibi, kamu kurum ve kuruluşların sunduğu hizmetlerde de; şeffaflık ve

verimliliğin artırılması, vatandaş odaklı ve ortak çalışmaya dayalı teknolojilerin kullanılması doğrultusunda çalışmaların hız kazanmasını sağlamıştır. Önceki bölümlerde c-devlet olarak adlandırılan bu girişim ve politikaların kamu kurum ve kuruluşlarında uygulanmasının önünde çeşitli zorluklar bulunmaktadır. Dinamik bir şekilde artan e-hizmet ihtiyaç ve taleplerine cevap verilebilmesi için gerekli kamu bütçelerinin kısa vadede temininin zorluğu ile birlikte; hedef kitlenin ilgili hizmetleri ne oranda benimseyip kullanacağını tahmin etmenin güç olması, ilgili hizmet altyapısı için optimal bilişim kaynağı planlamasını zorlaştırmaktadır. Bu durum, sadece belli hizmet veya hizmetler için tahsis edilecek bilişim kaynaklarına yapılacak düşük bütçeli yatırımın, çok kısa bir süre içinde bu bilişim kaynaklarının yüksek hizmet talebine cevap veremeyeceği; çok yüksek bütçeli yatırımın ise, uzun bir süre içinde yatırım yapılan bilişim kaynaklarının bir kısmının atıl kalacağı anlamına gelmektedir. Yine c-devleti destekleyen bilgi ve iletişim teknolojisinin çok hızlı ilerlemesi, yatırım yapılan kaynakların hızla demode olmasına yol açabilir.

Bu bilişimin c-devlet mimarisinde kullanımı bu sorunların çözümüne yönelik önemli faydalar sağlar. Bunun yanında daha az bakım maliyeti, güvenilirlik ve kullanılabilirliğin artışı gibi ek faydaları da mevcutttur. Bulut bilişimin kamu hizmetlerinin sunulmasında sağlayacağı faydaları şu şekilde sıralayabiliriz:

Kaynak havuzu: Geleneksel mimarilerde, her kuruluş veya birim normalde kuruluş veya birim tarafından özel olarak kullanılan bir veya daha fazla bilişim kaynağına sahiptir. Bulut bilişimde, bulut bilişim servis sağlayıcısına ait çeşitli bilişim kaynakları, birden çok müşteriye hizmet vermek üzere; hem servis sağlayıcı ve hem de müşterilerine uygun modellere dayalı bir şekilde bir havuzda toplanmaktadır. Servis sağlayıcı müşteri ihtiyaçlarına göre kaynak tahsis etmekte ve talep üzerine tahsisi yeniden ayarlayabilmektedir. Genel olarak müşteriler, hangi tür kaynakların kullanıldığına veya veri ve hizmetlerin nerede depolandığına veya üretildiğine dair hiçbir bilgiye sahip değildir. Servis sağlayıcısının belirli bir zamanda daha fazla kaynak gerektiren uygulamaları desteklemek veya farklı uygulamalara paylaştırmak için kaynaklarını bir havuzda topladığı kaynak havuzu özelliği, c-devlet için çok uygundur. Örneğin, son

ödeme tarihine yakın zamanlarda, vergi ödemelerini tamamlamaya çalışan vatandaş ve işletmelerde bir dalgalanmanın yaşandığı online vergi ödeme uygulamalarında, kolayca havuzdaki bilişim kaynakları tahsis edilebilmektedir (Mell, 2011).

Maliyet tasarrufu: BT kaynaklarının temini ve bunların bakımı için daha az sermaye yatırımı yapılması, ciddi oranda maliyet tasarrufları sağlamaktadır. Bulutun BT kaynak miktarına bakılmaksızın, açık bulut mimarilerindeki maliyet tasarruf oranı özel bulutlar göre daha fazladır. Kamuda bulut bilişim çözümlerinin kullanımının maliyet tasarrufu sağladığını teyit eden çok sayıda çalışma vardır. Örneğin, bulut bilişimin, yüksek kullanım, enerji tasarrufu ve yüksek kullanılabilirlik gibi diğer yararları yanında, mali geri ödeme sunduğunu belirtilmektedir (Golden, 2009). Kamu hizmetlerinin buluta aktarımının yüzde 25 ila 50 arasında bir maliyet tasarrufu sağladığı tahmin edilmektedir (West, 2010). Bazı ülkelerin bulut mimarilerini benimsemesi, milyarlarca dolara tekabül eden muazzam maliyet tasarrufları yaratabilir. Örneğin ABD'nin kamu hizmetlerinin buluta aktarımından (özellikle PaaS için), yılda 20 milyar dolar tasarruf sağlayabileceği düşünülmektedir (McKendrick, 2013a).

Ölçeklenebilirlik ve esneklik: Geleneksel bilişim sistemleri, kuruluşların kendi bilişim kaynaklarını bulundurmasını zorunlu kıldığından, kuruluşların bilişim kaynaklarına yatırım yapması gerekir. Bu yatırımın akıllıca yapılması gerekir, zira bilişim kaynağına yatırım, ancak ve ancak bu kaynağın verimli kullanılabildiği sürece kendini amorti edebilecektir. Kaynak miktarının yükseltilmesi durumunda, çoğunlukla yeni kaynaklar tamamen eskisinin yerini almakta ve önceki kaynaklar boşa çıkıp ciddi şekilde atıl kalmaktadır. Bu mimarilerde normalde yükseltme hızlıca yapılamaz; dolayısıyla esneklikleri düşüktür ve dolayısıyla aşağı ve yukarı ölçeklendirme kolayca yapılamaz.

Bulut bilişim, kaynakların kullanımı açısından farklı bir model sağlar. Kuruluşlar yatırım yapmak yerine yalnızca uygun modelleri kullanarak, bilişim kaynak ihtiyaçları için, bulut sağlayıcılarından dış kaynak sağlayabilir ve sadece kullanım başına ödeme yöntemini kullanarak, kullandıkları kaynaklar için ödeme yapabilirler. (Almunawar, 2014).

Esneklik, gerektiğinde kullanıcı kaynaklarının aşağı ve yukarı yönlü ölçeklendirilebilmesi anlamına gelir. Servis sağlayıcılardan, sözleşmeye göre tahsis edilen kaynakların yukarı veya aşağı yönlü ölçeklendirilmesi talep edilebilir veya bazı durumlarda ihtiyaca göre bunun otomatik olarak yapılması istenebilir. Bu durum, bir kuruluşun küçük ölçüde kaynağı kiralamaya başlayarak, gerektiğinde bunu büyütebilmesini mümkün kılar.

Kamuda çeviklik: Çeviklik, dinamik bir şekilde değişen ortam şartlarına hızlıca uyum sağlayabilmek için, hızlı ve etkin bir şekilde değişebilme yeteneği olarak tanımlanabilir. Kamusal alanda çeviklik kuruluşların; kısa vadede vatandaşların ihtiyaçlarını hızlı bir şekilde anlaması ve karşılaması, orta vadede eğilimlerine ve sorunlarına yönelik stratejik uyumu gerçekleştirmesi ve uzun vadede bütün bu girişimlerini şekillendirmesi yeteneğidir (Parker, 2008). Burada ilk adım vatandaşların ihtiyaçlarına hızlı tepki vermek, her zaman ve her yerden erişilebilir, uygun ve verimli hizmetler sunmaktır. Geleneksel bilişim sistemlerini kullanarak buna imkân veren c-devlet uygulamaları geliştirmek; yatırım bütçe kısıtları ve hizmetin sunumu için gerekli zaman açısından sorunlara yol açabileceğinden pek kolay değildir. Oysa bulut bilişimle, bilişim kaynakları dakikalar içinde toplanabilir ve geleneksel bilgisayardaki gibi haftalar veya aylar yerine, taşınabilir uygulamalar hızlı bir şekilde geliştirilebilir, internet üzerinden kullanılabilir ve her zaman ve her yerden çeşitli cihazlar kullanılarak erişilebilirler.

İhtiyaca göre bilişim kaynaklarının bir bölümü, vatandaşların talebine göre, hizmetleri hızlıca sunmak için bir bulut bilişim servis sağlayıcısından kiralanabilir. Bu sağlayıcı bir özel sektör firması olabileceği gibi, bir kamu bulutu sağlayıcısı kuruluş da olabilecektir. Kaynakların artırılması, bulut sağlayıcının bilgilendirilmesiyle kolayca ve hızlı bir şekilde gerçekleştirilebilir. Bu sayede hizmet düşük maliyetle başlatılabilir ve vatandaşların olumlu geri dönüşlerine göre hızlı bir şekilde genişletilebilir. Artık c-devlet ekibi, kısa vadede vatandaşlara genişleyen ve gelişen hizmetlerinin sunumu ve sonrasında uzun vadede bir strateji geliştirilmesi, vatandaş eğiliminin yönlendirilmesi, yeni fırsatlar yaratılması, olası sorunların tahmini ve önlenmesi de dâhil olmak üzere stratejik uyuma odaklanabilir. Özetle bulut mimarileri, bilişim kaynaklarının hızla

sağlanması, hizmetlerin düşük maliyetle başlatılabilmesi ve dinamik bir şekilde herhangi bir zamanda ölçeklendirilebilmesi yoluyla c-devletin çevikliğini artırır.

Güvenilirlik ve kullanılabilirlik: Kamu kuruluşlarının sunduğu c-devlet hizmetleri, internet aracılığıyla erişilebildikleri sürece, her zaman ve her yerde kullanılabilirler. Kuruluşlar herhangi bir hizmeti çalıştırmak için, normalde bir kurum içi veri merkezinde çalıştırılan veritabanlarına ihtiyaç duyarlar. Ancak hizmetin vatandaşlarca kullanımı, hizmet reddi (DoS) saldırısı gibi güvenlik tabanlı sorunların yanında; disk hataları, elektrik kesintisi veya sadece sistemin çökmesi gibi güvenlik tabanlı olmayan sorunlar nedeniyle aksayabilir. Hizmetlerin güvenilirliğini artırmak ve kesintileri önlemek için, yedekli veri merkezlerine ihtiyaç duyulur. Ancak bunların kurulumu çok yüksek bütçeler gerektirmektedir. Bir bulut bilişim servis sağlayıcısı, müşterileri üzerinde itibarını korumak için, verdiği hizmetin yüksek güvenilirlik ve kullanılabilirliğe sahip olduğunu garanti edebilmelidir. Bulut bilişim mimarisi farklı lokasyonlarda konumlandırılmış onbinlerce sunucuyu desteklendiğinden, yüksek güvenilirlik ve kullanılabilirliğe ek olarak; felaket kurtarma ve veri kurtarma da kolayca gerçekleştirilebilir.

Talep üzerine self-servis: Geleneksel bilişim mimarilerinin aksine bulut bilişimde, müşteri gereksinimlerine göre depolama boyutu veya işlem gücü gibi kaynakların miktarı, herhangi bir insan etkileşimi olmadan otomatik olarak ayarlanabilmekte, müşteriler gelecekte bu ayarı değiştirebilmekte ve böylece edinecekleri hizmetin miktarını belirleyebilmektedirler. Bulut bilişimin bu özelliği c-devlet için çok uygundur çünkü kamu sektörünün gereksinimleri dinamik olarak değişebilmekte ve herhangi bir aşamada ölçülmesi zor olabilmektedir. Hizmet kullanıcılarının dalgalanması beklenenden daha erken gelebilir ve bu durumla bulut bilişim mimarisinde kolayca başa çıkılabilir (Mell, 2011).

Basitlik: Ucuz istemci cihazlar haricinde bilişim kaynaklarına sahip olmayan bir kuruluş için, geleneksel mimari ile karşılaştırıldığında bulut bilişim hizmet sunumunu daha basit hale getirir. Kaynaklar bulut sağlayıcısından dış kaynak sağlama yoluyla temin edildiğinden kaynakların yönetimi çok basittir. Yine ücretler kullanım başına ödeme

yöntemine dayandığından maliyetleme de çok basit olur. Kaynak her zaman kullanıma hazırdır ve gerekli kapasite müşterinin talebine göre hazırda tutulmaktadır. Bunun yanında, bilişim kaynağının bakımı bulut sağlayıcısının işidir ve sağlayıcı uygulamaların üzerinde koştuğu sanal bilişim kaynaklarını kolayca yedekleyip değiştirebildiğinden, bakım servis kesintisi olmadan yapılabilir. Bulut bilişimin kullanımının basitliği, kamu kuruluşlarının bilişim altyapıları ile uğraşmak yerine, vatandaşlara sundukları temel hizmetlerine daha fazla odaklanmalarına ve bulut tabanlı hizmetleri c-devlet üzerinden geliştirmeye devam etmelerine yardımcı olur.

Kesintisiz güncelleştirme: Teknoloji sürekli değişmekte ve gelişmekte olup, sunulan hizmetlerin performansını ve uyumunu artırmak için yeni teknolojilere göre güncellenmesi gerekmektedir. Ancak, bu yeni teknolojilere göre sistem yükseltme veya yeni bir sisteme geçme basit bir işlem değildir. Bu gibi bir aktarım için, sistemin belli bir süre için bir kapatılması ve yapılacak güncelleştirme sonrası test edilmesi gerekir ki; bütün bu işlemler hizmet kesintileri oluşturacaktır. Bulut bilişim ise yeni teknolojiye geçişte bu sorunlara çözümler üretir ve hizmet kesintisine gerek duyulmaz. Servis sağlayıcılar, kendi sistemlerini güncelleştirilmiş şekilde tutarlar ve sistem güncellemesinin hizmetlerinin aksamasına etkisi olmaz. Bulut tabanlı c-devlet sistemleriyle, yeni teknolojilere sorunsuz bir yükseltme sağlanabilir ve c-devlet hizmetleri bu güncellemeler sırasında kesintiye uğramazlar.

Ölçülebilir hizmet: Servis sağlayıcılar, kaynak kullanımı ve ücretlerini belirlemek için, müşterileriyle birlikte üzerinde anlaşmaya varılmış bazı ölçüm araçlarını kullanırlar. Servis kaynak kullanımı izlenir, kontrol edilir, ölçülür ve her iki taraf için rapor edilir. Bu durum, kamu sektörüne kullanım ve kullanımın zirve yaptığı zamanlar için bir ölçüm sağladığından, c-hükümeti desteklemektedir (Mell, 2011).

Küresel erişim: Bulut bilişim kaynakları internet üzerinden erişilebilir ve bu erişim konum ve platform bağımsızdır. Vatandaşlar ortak bir arayüz kullanarak, her zaman ve her yerde uygulamalara erişebilirler. Mobil erişimin sağlanması, mekân bağımsız olarak her yerden erişimi mümkün kılar. İletişim ve işbirliğini sağlamak amacıyla eşzamanlı

erişim kolaylıkla gerçekleştirilebilir. Bu sayede örneğin, ekip çalışması yapan bir grup insan, farklı yerlerden aynı anda bir proje üzerinde çalışabilirler. Burada hizmet gecikmesini önlemek için, internet hızının hizmetin iyi bir şekilde sunulabilmesine olanak sağlayacak kabul edilebilir bir düzeyde olmasına dikkat etmek önemlidir. Internet genişbant erişiminde yaşanan hızlı gelişme ve iyileştirmeler, bulut tabanlı c-devlet mimarilerini son derece uygulanabilir kılmaktadır.

Yeşil teknoloji: Geleneksel mimarilerde kamu kuruluşları, c-devlet sistemi üzerinden süreçleri ve çeşitli hizmetleri gerçekleştirmek için çeşitli veri merkezlerine ihtiyaç duyarlar. Ayrıca sistemin güvenilirliğini artırmak için, yedekli veri merkezi mimarisi kurmak zorunlu hale gelmiştir. Ancak bu veri merkezleri çok miktarda enerji tüketirler ve daha fazla veri merkezi daha fazla güç tüketimi anlamına gelmektedir. Çok sayıda hizmeti işletmek amacıyla bir araya toplanmış ve bu hizmetler tarafından paylaşılan kaynaklar toplam enerji tüketimini azaltacaktır. Bu sayede kamu kuruluşları güç tüketiminden tasarruf edecek ve bu sürdürülebilir gelişimlerine devam edebileceklerdir. Kuruluşların, enerji tüketimlerini azaltmak için bulut bilişimi benimsenme eğiliminde oldukları yapılan birçok çalışmada gösterilmiştir. Uygulamaların buluta aktarılmasının kuruluşlara sağlayacağı enerji tasarrufu oranının % 90'dan fazla olabileceği tahmin edilmektedir (McKendrick, 2011).

2.6.2. Kamuda Bulut Bilişim Kullanımına Yönelik Sorunlar

Herhangi bir teknolojik girişimde olduğu gibi, bulut bilişimde de; aktarım ve kullanım sırasında yaşanan birçok zorluklar vardır ve c-hükümet için bulut bilişimin benimsenmesi sürecinde bu zorluklara dikkat edilmelidir. Bazı önemli zorluklar aşağıda vurgulanmaktadır:

Güvenlik ve gizlilik: C-devlet için kamu sektörünün temel önceliklerinden biri, gerektiği kadar katmanda yüksek güvenlik seviyeleri sağlayarak, hizmetleri güvenilir şekilde sunabilmektir. Ancak birçok ülkede, servis sağlayıcıların makinelerinde veri depolama ve uygulamaları çalıştırma ile ilgili güvenlik sorunlarına dayalı müşteri

kaygıları sebebiyle, bulut bilişimin benimsenmesi gecikmektedir. Veri kaybı, kimlik avı ve botnet (çok sayıda bilgisayarın bir IP'ye saldırması) gibi en bilinen sorunlar nedeniyle bu endişeler ortaya çıkmaktadır. Yine bulut bilişimin yeni çoklu kiralama modeli ve bilişim kaynaklarının ortak havuzda toplanmasının, kullanıcıları karşı karşıya getirdiği diğer güvenlik zorlukları da vardır (Kuyoro, 2011). Bu zorluklara kuruluşların verinin sağlayıcı tarafından nasıl ve nerede saklandığına dair herhangi bir bilgiye sahip olmaması sebebiyle, veri veya bilgilerin kontrolünün kaybı neden olmaktadır. Bu sorunu aşmak için, birçok ülke verileri güvenceye almak ve korumak için, kullanılan kurulum ve altyapı üzerinde daha fazla kontrol sağlayan, özel veya topluluk bulutu mimarilerini kullanmaktadır.

Ekonomik sorunlar: Bulut bilişimin maliyet tasarrufu sağlayacağına ilişkin birçok çalışma gösterilebilir ancak konuya farklı bir perspektiften bakan çalışmalar da vardır. Hemen bütün araştırmalara göre ilk kurulum maliyeti, uygulama maliyeti ve bakım maliyeti açısından sağladığı tasarruf; bulut bilişimi c-devlet için kullanılması yönünde desteklemektedir. Ancak, 2009 yılında IDC tarafından yapılan bir anket, kullanıcıların bulut bilişimin kendilerine daha pahalıya mal olacağı endişesini taşıdıklarını göstermektedir (Gens, 2009). Bu endişeler, kullanıcıların kendilerine ayrılan bütçeden daha fazla maliyete sahip kaynak kullanmak durumunda kalırlarsa ne olacağı düşüncesine dayanmaktadır. Buluta aktarımın altyapı maliyetlerini azaltacağı görülmektedir fakat özellikle açık, topluluk ve hibrit bulut için veri trafiği maliyeti artabilecektir. Bu sebeple kamu kuruluşlarının geliştirecekleri iş modeline göre, çeşitli bulut bilişim mimarileri üzerinde detaylı maliyetlendirme çalışmalarına (toplam kaynak sahip olma maliyeti ile karşılaştırmalı) ihtiyaçları vardır (Kuyoro, 2011).

Veri koruma ve uyum: C-devlette genellikle hassas veriler işlenmekte veya iletilmekte olup, bu durum veri korumayı önemli bir etmen haline getirmiştir. Bazı ülkelerde mevzuat, bir ülkenin verilerinin başka bir ülkeye hareketine izin vermez. Bu sebeple, servis sağlayıcıların bu düzenlemelere uyumlu olması gerekir. Ancak sağlayıcıların farklı ülkelerdeki işletme açısından düşük maliyetli sunucu çiftlikleri ve veri merkezlerini kullanma eğilimi yasal sorunlar ortaya çıkarmaktadır. Bu durum

kullanıcıların; yargı, veri koruma, adli bilgi uygulamaları (FIP) ve uluslararası veri transferi ile ilgili endişe duymalarına neden olur (Lewis, 2013). Servis sağlayıcıların, daha ucuz veya daha güvenli yerleri bulmak veya felaket kurtarma amaçları için, genellikle dünya genelinde veri merkezlerine sahip olmaları, devletin bulut bilişimi benimsemesi önündeki büyük bir sorundur (özellikle açık bulut için). Verilerin oluşturulmasından dağıtımına kadar, tüm olası tehditlere karşı uygun şekilde korunması gerekmektedir. Avrupa'da ülkeler, sadece ilgili ülkede veri depolamak için kamu bulutları kurma lehine tavır almış ve genellikle açık bulutlardan kaçınmışlardır (Zwattendorfer, 2013b).

Birlikte çalışabilirlik ve veri taşınabilirliği: Bu zorluklar genellikle, müşterinin zaten bir servis sağlayıcının kaynaklarını kullandığı ve daha iyi hizmet veya ücretleri sunabilen diğer servis sağlayıcılarını bulsa bile, veri ve uygulamalarını bu yeni sağlayıcıya aktarmasında yaşaması muhtemel zorluklar nedeniyle, mevcut sağlayıcıya bağımlı kalması sebebiyle ortaya çıkar. Çözüme yönelik olarak, standarlaştırılmış hizmetler ve arayüzler, servis sağlayıcıları arasında birlikte çalışabilirliği destekleyecektir. Yapılan çalışmalar bulut sağlayıcıların, müşterileri ellerinde tutabilmek için, farklı bulut ortamlarında birlikte çalışabilirliğin ve veri taşınabilirliğinin gelişmesini engelleyen, kendi özel yöntemlerine sahip olduğunu göstermektedir. Bulut topluluğunun takip edebileceği, tanımlanmış standartlar setine sahip olunmaması sağlayıcıya bağımlılık riskine yol açmaktadır (Lewis, 2013). Yine kişiye özel bulut API'leri, mevcut eski sistemler ile bulut hizmetlerinin entegre olmasını zorlaştırmaktadır. Birlikte çalışabilirlik ve veri taşınabilirliğini sağlamak için birçok ülke açık kaynak bileşenleri kullanmakta ve kendi kamu bulutları içinde açık kaynak standartları uygulamaktadır (Zwattendorfer, 2013b).

Hizmet Seviye Anlaşmaları (SLA): Hizmet veya verilerin servis sağlayıcıya aktarılması sürecinde; kalite, kullanılabilirlik, güvenilirlik ve kaynak performansı sağlamak için, bu anlaşmanın kamu kuruluşları tarafından bizzat yapılması gerekmektedir. Burada sorun, farklı kamu kurum ve kuruluşlarının güvenlik, veri mahremiyeti ve verilerin korunması gibi alanlarda farklı gereksinimlere sahip olması ve

sağlayıcıların bu gereksinimlerle ilgili dengeyi sağlamakta yaşadığı zorluklardır. Servis sağlayıcının kaynak tahsis mekanizması, farklı bulut teklifleri ve müşterileri için doğrulanan, değerlendirilen ve uygulanan farklı kamu ihtiyaçlarını karşılamak zorundadır ve bu durum sağlayıcılar açısından uygulama sorunlarına neden olabilmektedir (Zwattendorfer, 2013b).

Kimlik ve erişim yönetimi: C-devlet hizmetleri ve uygulamaları genellikle, çok güvenli ve güvenilir bir kimlik saptama ve doğrulama yöntemine gereksinim duyarlar fakat geçerli bulut uygulamaları hala bu alanda eksiktirler. Farklı uygulamalar üzerinde aynı kişilerin farklı hesaplara, kullanıcı rol ve yetkilerine sahip olması, hem kuruluşlar ve hem de sağlayıcılar açısından hizmetleri yönetmeyi zorlaştırmaktadır. Bu zorluğu aşmak ve c-devlet gereksinimlerini karşılamak amacıyla, bu hizmetleri sunmaya başlayan bazı sağlayıcılar vardır.

Denetim: Servis sağlayıcılar henüz, kuruluşların verilerinin ve uygulamalarının mevzuata ve Hizmet Seviye Anlaşmalarına uygun şekilde tutulup tutulmadığına dair detaylı denetim olanakları sunmamaktadırlar. C-devlet için spesifik politikalar ve düzenlemelere uyacak şekilde ve bulut bilişimin benimsenmesine yönelik ihtiyaçları karşılamak amacıyla, bu konuda daha fazla araştırma ve geliştirme yapılması gereklidir.

Buluta aktarım: Bu zorluk, bulut bilişimin yaygın olarak sağlanması ve desteklenmesi için hala tanımlanmayan bulut standartları nedeniyledir. Buluta aktarımın da bir maliyeti vardır ve bu maliyetin boyutu, kaynak ve hedefin benzerlikleri ve farklılıklarına göre değişmektedir. Bulut servis sağlayıcılarının c-devlet hizmetleri için birkaç standart platformu olacak olsa da, hala sağlayıcı tarafından desteklenmeyen ve c-devlet üzerinde çalışan hizmetler var olabilecektir. Bulut standardizasyonunda farklılıkları azaltmak için; kullanıcı kimliği, iş yükü (sanal makine görüntüleri), bulut depolama API'leri ve bulut yönetim API'leri gibi bazı ortak konular üzerinde çalışılmalıdır. Bu nedenle, bunların her biri üzerinde bir uzlaşma, aktarım çabalarını azaltabilir ve dönüştürücü, içe aktaran, dışa aktaran, ya da soyut API'lerin oluşturulmasını sağlayabilir (Lewis, 2013).

2.7. Kamuda Bulut Kullanımı İle İlgili Modeller ve Çözüm Önerileri

Bu bölümde öncelikle bulut bilişim teknolojilerinin kamu sektöründe en çok kullanıldığı alanlara ilişkin modeller ve geleneksel bilişim mimarilerinin yerine bu modellerin kullanılmasının ilgili kamu kuruluşlarına sağladığı getiriler üzerinde durulacaktır. Sonrasında ise, Avrupa Birliği üyelik sürecinde bulunan ülkemiz için, bulut bilişimin benimsenmesi ile ilgili kilometre taşları oluşturabilecek olan ve Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından güvenli kamu bulutları kurulmasına yönelik ortaya konulan tavsiye ve çözüm önerileri açıklanacaktır.

2.7.1. Kamuda Bulut Kullanımı İle İlgili Modeller

2009 yılında Avrupa genelinde bulut bilişimin farklı endüstriyel sektör ve hizmetlerde kullanım oranlarının belirlenmesine yönelik yapılan bir ankete göre; bulut bilişim teknolojileri en çok finansal hizmetler (% 12), iş ve yönetim sektörü (% 10), endüstriyel üretim (% 10), telekomünikasyon (% 9), kamu yönetimi (% 7), sigortacılık (% 6), mesleki hizmetler (% 6), eğitim (% 4) ve sağlık (% 4) vb. alanlarda kullanılmaktadır (Pettey, 2009). Bu alanlardan kamu kuruluşlarının görev alanına giren başlıcaları ile ilgili kullanım modelleri ve bu modellerin kuruluşlara getirdiği avantajlar şu şekildedir:

Finansal Hizmetlerde Bulut Bilişim Modeli: Günümüzde finansal hizmetler sektörü, pazarı etkileyen çok sayıda sorunla karşı karşıyadır. Sürekli artan müşteri beklentileri, büyük veri kullanımı, değişen uyum şartları ve bilgi güvenliği tehditleri bunlardan sadece birkaçıdır. Önemli seviyede BT servislerine dayanan bir finansal hizmet şirketi, bulut bilişim hizmetlerinden etkin bir şekilde yararlanabilir. Maliyet tasarrufu, içeri ve dışarı yönlü ölçeklendirme kolaylığı, hizmetleri müşterilerine daha hızlı sunma imkânı, şirket çapında bir hizmet olarak veri sanallaştırma, kurumsal teknolojilerde standardizasyon ve hareket halindeyken veri ve uygulamalara erişme yeteneği finansal hizmet firmalarını bulut bilişimi benimsemeye teşvik eden kritik faktörlerdir.

Çeşitli uygulamalarını aktararak bulut bilişimden faydalanma adına, finansal hizmet firmalarının sayısız fırsatları vardır. İşe alma, faturalama ve kuruluş çapında seyahat yönetimi gibi temel olmayan uygulamaları ve iş süreçleri kolayca buluta taşınabilmektedir. Veri merkezi yönetimi, veri depolama ve felaket kurtarma gibi bir dizi altyapı işlemleri, farklı sağlayıcıların tekliflerinin ayrıntılı bir değerlendirmesi sonrasında, sözleşmeleri hazırlayan bulut sağlayıcısının esnekliğine dayalı olarak buluta aktarılabilir. Çok az sayıda şirket şu aşamada kendi temel uygulamaları için bulut bilişim kullanıyor olsa da, Servis olarak Altyapı (IaaS) bulut sağlayıcılar tarafından sağlanan farklı barındırma mimarileri ile topluluk ve hibrit bulut mimarilerindeki yeni uygulamalar; daha fazla firmayı temel uygulamalarını buluta taşıma konusunda teşvik edecektir. Aslında, gün boyu çalışan toplu iş süreçleri gibi, analitik ve raporlama uygulamaları, bu temel uygulamalara mükemmel adaylardır (Garg, 2011). Veri güvenliği ve gizliliği, uyum, kullanılabilirlik ve sağlayıcılar arasında tanımlı standartların eksikliği (sağlayıcıya bağımlılık), bulut bilişimin daha fazla benimsenmesine engel olan temel etmenlerdir.

Kamu Yönetimi Alanında Bulut Bilişim Modeli: Günümüzde bulut bilişim teknolojilerinin kamu hizmet ve uygulamalarında kullanımı, giderek yaygınlaşmakta ve önem kazanmaktadır. Kamu hizmetlerinin birçoğunun farklı kamu kuruluşlarının servis ettiği uygulamalarla entegre bir biçimde çalışma zorunluluğu, bulut bilişimin benimsenmesinde rol oynayan önemli bir faktördür. Bulut bilişimin kamusal veriyi, sadece o veri için tahsis edilmiş sunuculardan çıkarıp, yetki dâhilinde her yerden erişilebilecek şekilde sunması; farklı uygulama ve hizmetlerin ilgili veriyi ortak bir şekilde kullanabilecek biçimde entegre olmasına imkân tanımaktadır. Örneğin birçok e-devlet uygulaması, kişi bazlı hizmet verebilmek için hizmeti talep eden vatandaşın nüfus verilerine ihtiyaç duymaktadır. Bulut bilişim, bu verileri yetki sahibi diğer kamu kuruluşlarının erişebileceği şekilde kamuya açmayı çok basit hale getirmektedir. Aynı verileri kullanacak her bir uygulama için ayrı ayrı web servisler yazmak yerine, tek bir web servis şablonunda, verinin sadece ihtiyaç duyulan kısmının tanımlanarak aktarılması sağlanabilmektedir. Yine vatandaşların enerji, su ve doğalgaz gibi

tüketimlerinin faturalandırılmasında veya emlak, kültür varlıkları koruma vergisi vb. vergilerinin hesaplanmasında tapu kayıtlarının kullanılması, entegre hizmete diğer bir örnektir. Yine kamu kuruluşlarının personel kayıtlarının tutulması, maaş ve özlük işlemlerinin ilgili kamu kuruluşu ve kamunun personel rejiminden sorumlu Devlet Personel Başkanlığı ve Maliye Bakanlığı gibi kuruluşlarla eşgüdümlü olarak yapılması konularında, bulut bilişim önemli bir esneklik sağlamaktadır. Kamu harcamaları ile ilgili muhasebe kayıtları bu duruma diğer bir örnektir. Bulut bilişimin hizmet tabanlı yapısı ayrıca, belediyeler için kent rehberi, adres, arazi kullanımı, e- imar, trafik ve yol durumu, toplu taşıma vb. gibi harita tabanlı ve büyük veri altlığı gerektiren kent bilgi sistemi uygulamalarının işletilmesi ve bu uygulamaların işletilmesi için gerekli coğrafi veri altlığının temini için önemli fırsatlar sunmaktadır. Servis olarak Altyapı (IaaS) mimarisi, bilişim kaynağı temin etme konusunda yeterli kaynağa, zaman veya tecrübeye sahip olmayan kamu kuruluşlarına, bu kaynakları kiralama yoluyla temin etme imkânı sunarken; Servis olarak Platform (PaaS) mimarisi sayesinde, farklı kamu kuruluşlarında ve özellikle de farklı belediyelerde aynı tür hizmetler için kullanılan uygulamaların, ilgili kamu kuruluşu tarafından kendi görev alanına göre geliştirmesine imkân tanıyan şablon uygulama ve hizmetler bulutta kolayca işletilebilmektedir. Yine veri mahremiyeti konusunda yasal kısıtlamalar içermeyen uygulamalar için, bulut servis sağlayıcılarının sunduğu yazılım uygulamalarının kiralanması (Servis olarak Yazılım (SaaS)); kamu kuruluşlarına ciddi maliyet, zaman ve hizmet kalitesi avantajları sağlamaktadır.

Telekomünikasyon Hizmetlerinde Bulut Bilişim Modeli: Telekomünikasyon sektöründe bulut bilişim, ağ donanımı ve servis sağlayıcılarının her ikisi için de, hem operasyonel verimlilik için temel teknoloji ve hem de yeni iş imkânları anlamına gelir. İç verimliliği artırmak için geleneksel faydalarının ötesinde, bulut bilişim teknolojileri ürün tabanlı bir modelden servis tabanlı bir modele geçişi sağlamaktadırlar. Bir Sevis olarak Yazılım (SaaS) modeli, geleneksel telekom altyapı özelliklerinin yanında; teslim süreleri, esneklik ve düşük işletme maliyetleri açısından önemli yararlar sağlar. Telekomünikasyon sektörü kuruluşları, güvenlik altyapısı ve hizmet kalitesi gereksinimleri için bulut bilişim teknolojilerini kullanılabilirler. Bulut bilişim üzerine

bugüne kadar yapılan araştırma ve uygulamalar; bir araya toplama, sanallaştırma ve ölçek ekonomileri yoluyla maliyetleri aşağı çeken etkileyici sonuçlarıyla; işlem ve depolama kaynaklarının talebe bağlı servisine odaklanmıştır. Ancak ağ, güvenlik ve bazı uygulamaların gerektirdiği hizmet seviyesi anlaşması şartlarının yerine getirilmesi ile ilgili çeşitli temel konular henüz tam olarak ele alınmamıştır.

Barındırılan ve yönetilen hizmet yaklaşımları ile Servis olarak Yazılım (SaaS) modeli arasında büyük farklar bulunmaktadır. Bu farklılıklar iş modelleri ve çalışma modları ile alakalıdır ama aynı zamanda önemli teknolojik etkenler de bulunmaktadır. Servis olarak Yazılım (SaaS) mimarisi, kullanım talepleri dalgalanan ve maliyet özellikleri değişen bazı telekom hizmetleri için, büyük ölçekli ilk yatırım eksikliği nedeniyle oluşabilecek maliyetleri kontrolü altında tutmaya yardımcı olup, maliyet riskini azaltan ve aynı zamanda, hizmetin hızlı bir şekilde kurulup, son kullanıcılara sunulmasını kolaylaştıran bir yaklaşım sağlar. Bu mimari birkaç teknik zorluğu da beraberinde getirmektedir. Birçok telekom hizmetinin ve gerçek zamanlı hizmetin temel özelliklerinden biri, uçtan uca bazı performans özelliklerinin sağlanmasının gerekliliğidir. Bu tür gereksinimlerin, bulut mimarisi içinde performans garantilerinin sağlanması için, gerekli hizmet seviyesi anlaşmalarında düzenlenmeleri gerekir. Telekom sektöründe Servis olarak Yazılım (SaaS) mimarisinin diğer bir zorluğu da çoklu kullanıcılarla ilgilidir. Geleneksel telekom altyapısında yazılım, aynı kaynaklar için rekabet eden diğer uygulamaların müdahalesi olmaksızın, kendisi için tahsis edilmiş donanım üzerinde çalıştırılır. Ancak bulut bilişim bağlamında, bu artık geçerli olmayıp, aynı altyapı üzerinde çalışan birden fazla telekom ağı bulunabilir. Bu sebeple, bulut kiracıları arasında performans veya güvenlik açılarından birbirine müdahalenin olmayacağı güçlü izolasyon özelliklerinin garanti edilmesi gerekir (Vajda, 2015).

Eğitimde Bulut Bilişim Modeli: Öğrenciler, eğitim görevlileri, okul yönetimi ve diğer idari personel ile eğitim içeriklerini hazırlayan özel firmalar gibi çok çeşitli rollerdeki kullanıcının bulunabileceği eğitim bulutları, kamuda bulut bilişimin efektif şekilde kullanılabileceği alanların başındadır. Tüm bu ana kullanıcıların her biri için roller atanabilmekte ve atandığı rol bazında erişim imkânı sağlanabilmektedir. Öğrenciler,

öğretmenlerinin sağladığı tüm öğretim materyaline zaman ve mekân bağımsız olarak bilgisayarlarını veya diğer elektronik cihazlarını kullanarak internet üzerinden erişmeleri mümkün olacak şekilde; bulut sunucuları üzerine kendi konu anlatımı, ödev ve testlerini yükleyebilirler. Eğitim sistemi öğretmenlerin, öğrencilerinin çalışma kayıtlarını analiz ederek, hata yapma eğiliminde oldukları konuları tespit etmesini mümkün hale getirecektir. Yine öğrencilerin, ders sırasında çevrimiçi öğretim materyallerini kullanmaları yanında; bu materyallere, derslere hazırlanmak ve ders tekrarı yapmak için, evden de erişimleri mümkün olacaktır. Bulut bilişim sistemlerinin kullanılması, sunucular ve öğrenme materyallerinin geleneksel dağıtım modelindeki diğer okullar ile paylaşılabilmesine ve tüm bilgi teknolojisi kaynaklarının tek bir sistemin içinden yönetilebilmesine imkân tanıyacağından, operasyon maliyetlerini azaltacaktır. Bu hizmetler ve araçların birçoğu, kolayca buluta aktarılabililer ve internet üzerinden ya da tamamen işlevsel uygulamalar (SaaS), geliştirme platformları (PaaS) veya ham bilişim kaynakları (IaaS) olarak doğrudan kullanılabilirler. Eğitim alanında bulut mimarisi kullanımının sağladığı araç ve faydalardan bazıları şunlardır:

- Çevrimiçi ders dağıtım platformları sunulması,
- Çevrimiçi ödevler ve testler sunulması,
- Proje üzerinde işbirliği ve birlikte çalışabilirliğin artırılması,
- Derse katılımda artış,
- Raporlama araçları,
- Tasarım, modelleme ve araştırma kolaylığı,
- BT işiyle uğraşmak yerine eğitim içeriklerine odaklanma,
- E-posta, ses ve video işbirliği çözümleri,

Sağlıkta Bulut Bilişim Modeli: Sağlık alanında bulut bilişimin kullanımı, sağlık hizmetlerinin karşılanması hususunda zamanla anahtar rol oynar hale gelmiştir. Sağlık sisteminde elektronik tıbbi kayıtlar (EMR), elektronik sağlık kayıtları (EHR), kişisel sağlık kayıtları (PHR), entegre bakım teknolojileri, hasta güvenliği, hasta başına demografik ve klinik bilgi gibi verilerin entegre edilerek, erişime açılması bu alanda

istikrarlı büyümeye imkân tanımaktadır. Hasta ve hekimin bulunduğu yere bakılmaksızın verilerinin mevcudiyeti, hasta memnuniyetinin ve gelişmiş klinik sonuçların anahtarı haline gelmiştir. Bulut teknolojileri, bu eğilimi önemli ölçüde kolaylaştırmakta ve sağlık sektörüne önemli avantajlar sunmaktadır. Hekimlerin kendi klinikleri, hastaneler ve diğer sağlık klinikleri; çoklu bilişim kaynaklarına ve büyük veri merkezlerine hızlı erişim gerektirirken, geleneksel mimaride bu imkân sağlanamaz. Ayrıca, sağlık verileri çeşitli uygulamalar ve lokasyonlar arasında paylaşılması gereken veriler olup; bunların zamanında paylaşılmaması tedavide zaman kaybına ve önemli gecikmeye neden olur. Bulut mimarisi bu sebeplerle sağlık kuruluşlarına önemli fırsatlar sağlayıp, birçok gereksinimlerine hitap ederek; müşterilerine ve hastalara hizmet vermek, her zamankinden daha kolay bilgi paylaşmak ve aynı zamanda kuruluşun işlevsel etkinliğini artırmak anlamında faydalar sağlar. Sağlık alanında bulut mimarisi kullanımının sağladığı araç ve faydalardan bazıları şunlardır:

- Klinik araştırmalarda ortaya çıkan büyük veri setlerini işleme imkânı,
- Elektronik Tıbbi Kayıtlar ve bu kayıtların arşivleri,
- Video konferans üzerinden doktor muayeneleri,
- Telefon vasıtasıyla tedavi,
- Klinik ilaç denemeleri için genomik veriler, EHRs, radyoloji görüntüleri gibi büyük verilerin barındırılması,
- Kuruluşlar arasında sağlık bilgi değişimi,
- Tedavi, maliyet, performans ve etkinlik çalışmalarını analiz edebilecek araçlar.

2.7.2. Kamuda Bulut Bilişim Kullanımı İle İlgili Çözüm Önerileri

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA), Avrupa ülkelerinde bulut bilişimin benimsenmesine ilişkin Avrupa'daki mevcut duruma ve öngörülen senaryolara göre, güvenli kamu bulutları kurulmasına yönelik ortaya koyduğu tavsiye ve çözüm önerisi başlıkları şu şekildedir:

- Üye Ülkelerin (MS) ve Avrupa Komisyonunun (EC) kamu bulutlarının benimsenmesini sağlamak için, AB stratejisinin gelişimini desteklemeleri,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) kamu bulut çözümlerinin sürdürülebilirliğini ve ekonomikliğini garanti etmek için bir iş modeli geliştirmeleri,
- Üye Ülkelerin (MS) ve bulut sağlayıcılarının "kontrol kaybını" sorununu azaltmak için bir çerçeve geliştirilmesini teşvik etmeleri,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) "yerellik sorununu" çözmek için bir düzenleyici çerçevenin tanımını teşvik etmeleri,
- Üye Ülkelerin (MS) ve bulut sağlayıcıların, AB ve ülkeye özgü düzenlemeler ile uyumlu kamu bulut çözümlerinin geliştirilmesini teşvik etmeleri,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) bir Hizmet Seviye Anlaşması (SLA) çerçevesinin gelişimini desteklemeleri,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) açık ve özel bulut dağıtım modelleri için temel güvenlik önlemlerinin alınmasını teşvik etmeleri,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) bir sertifikasyon çerçevesi geliştirmeleri,
- Akademisyenler ve bulut sağlayıcıların, kamu bulutu güvenliği konusunda araştırmaya teşvik edilmesi,
- Avrupa Komisyonunun (EC) ve Üye Ülkelerin (MS) bulutta veri gizliliği artışını desteklemeleri,

Aşağıda bu önerilerin hem açıklamalarına ve hem de alınması gereken tedbirlere yer verilmiştir:

Öneri 1: AB kamu bulutu stratejisi

Kamu sektöründe bulut bilişimin benimsenmesi, Avrupa'da çok heterojendir. Bu yavaş benimsenme süreci; güvenlik, kontrol, veri koruma ve bilinçsizlik gibi birçok sebebe bağlıdır. Her ne kadar mevcut ya da önerilen güvenlik mevzuatları bilgi güvenliği gereksinimlerinden bazılarını kapsıyor olsa da, BT hizmetlerinin nasıl işletileceğinin farkında olmanın ve bulutun benimsenmesinin ne gibi güvenlik önlemi revizyonlarına sebep olacağını bilmenin, bulut bilişim kullanımı üzerinde önemli bir etkisi vardır. Çalışmalar kamu bulutunun sistematik bir şekilde benimsenmesinin, bulut bilişim benimsenmesini ele alan ulusal bir strateji sahibi ülkelerde, daha ileri düzeyde olduğunu ortaya koymaktadır. Ayrıca, sadece kamu sektörü ve kamuda bulut bilişim için ulusal stratejiler üzerine odaklanan bir AB stratejisinin geliştirilmesinin, AB ülkelerinde kamu bulutu benimsenmesini teşvik edeceği ile ilgili birçok uzman ikna olmuştur.

Tedbirler:

1- Teknik, hukuki ve kurumsal konuları kapsayan üst düzey ilkelerle ilgili ayrıntılı bir strateji tasarlamak.

2- Güvenli bulut hizmetlerinin çok büyük miktarda sunumunu; adım adım bir işletme planı, anlamlı çıktılar ve kilometre taşları belirleyerek planlayan bir program düşünmek.

3- Bulutu devreye almayı özendirecek ve kuruluşları cesaretlendirecek; bilgiye dayalı, risk temelli politikaların ve "açık veri" için harici açık bulut çözümlerinin kullanımını kamu sektöründe teşvik etmek.

4- Kamuda bilgi ve iletişim teknolojilerinin verimliliğini ve veri merkezi toplulaştırmasını artırmak için, proje ve girişimlerle ulusal bulut stratejisini ilişkilendirmek.

5- Kamu bulutu mimari seçeneklerini (açık, özel, topluluk ve hibrit), hizmetlerin türüne ve gizlilik, güvenlik ve kontrol gibi gereksinimlerine dayalı olarak değerlendirmek.

6- Üye Ülkelerin (MS) stratejilerinin; güvenlik ve verilerin koruması hakkındaki kanun, yönetmelik ve ulusal ajans şartlarına uyumlu olmasını sağlaması ve ayrıca verilerin gizliliğini dikkate alarak ulusal stratejinin; güvenlik, bilgi, varlıklar ve altyapıların korunması vb. ulusal ve AB kanun ve yönetmeliklerine uyumlu olduğundan emin olunması,

7- Kamu hizmet katalogları geliştirmek için; bulut ürünleri, uygulamaları ve hizmetlerine ait kataloglarını ve ayrıca hedefe yönelik kamu bulut platformlarının, kullanım profillerinin ve en iyi uygulamaların sınıflandırıldığı seçenekleri değerlendirmek.

Öneri 2: Sürdürülebilirliği garanti eden bir iş modeli

Bugün, AB kamu bulutlarında en yaygın şekilde özel bulut mimarisi kullanılmaktadır. Açık bulut mimarisinin kullanımının düşük kalması, açık bulut çözümlerinin mevzuata ilişkin zayıflıklarına ve gelişmemişliklerine dayanmaktadır. Açık bulut bilişim piyasasının göreceli gelişmemişliğinin ortaya çıkardığı üç önemli zorluk vardır:

1- Piyasada çok sayıda bulut bilişim hizmet sağlayıcısı bulunmasına rağmen, bunların çoğunun işe başlangıç seviyesinde olması ve bu nedenle kamu ile işbirliği yapabilecek bir şirketin sahip olması gereken istikrar seviyesini garanti edememeleri,

2- Çoğu çözümlerin belli bir iş bağlamında dizayn edilmesi ve bu sebeple piyasadaki birçok açık bulut çözümünün kamunun spesifik ihtiyaçlarına cevap verememesi,

3- Piyasada bugün veri koruması için kamunun özel sorumluluğunu göz önünde bulundurabilecek sadece birkaç çözümün mevcut olması,

Sonuç olarak hala piyasada göreceli olarak, bir devlet tarafından kullanıma uygun, çok az sayıda açık bulut bilişim çözümü vardır. Ancak, özel bulut inşa etmek, işletmek ve mevcut hizmetlerin bu buluta aktarılması pahalı olabilir. Gerçek maliyet tasarrufunu sağlayacak yetenekte bir maliyet modelinin geliştirilmesi zordur.

Kamu bulutunun benimsenmesini artırmak için, Avrupa Komisyonu ve Üye Ülkelerin yetkili makamlarının, bulut sağlayıcıları ile işbirliği içinde, verimliliği ve kamu bulut çözümlerinin ölçek ekonomisini garanti edecek bir iş modeli geliştirmeleri gerekir. Çözüm uygun bir, açık/topluluk bulut mimarisinin kullanılması yönünde hareket etmektir. Bu model veri ve hizmet kullanılabilirliği, hizmet güvenilirliği ve güvenliğini artırmak için yatırım maliyetlerini azaltacaktır.

Tedbirler: Çok kiracılı altyapı ve Üye Ülkeler arasında hizmet paylaşımının benimsenmesini sağlamak için bir düzenleyici çerçeve gereklidir. Bu çerçeve veri ve hizmet yerellik sorununu ele almalıdır. Çerçeve aynı zamanda bulut sağlayıcı değiştirme veya bulut hizmeti sonlandırma ile gelen sorunları da ele almalıdır. Burada bir Hizmet Seviye Anlaşması'nda olması gereken şart ve koşullar ile bu şartların ve koşulların uygulanabilirliği üzerinde durulmalıdır. İkinci olarak, bağımsız bir üçüncü taraf güvencesi, sağlayıcı ve müşteriler arasında güven inşasına katkıda bulunabilecek ve bu sayede Avrupa KOBİ'leri ve diğer kuruluşlar, bulut bilişim servislerini daha fazla kullanacaklardır. Ana fikir, devlet kurumlarının bulut satıcılarını akredite edecebileceği bir çerçeve kurmak ve bir üçüncü tarafça bir tür aktif ve etkin emanet hizmeti sunmaktır. Bu şekilde diğer tarafın bulut operasyonlarını kesintisiz devralması sağlanabilinir ve A bulut sağlayıcısı bir kullanıcı için B sağlayıcısına başvurabilir. Bu yazılım kullanıcıların verilerinin ve işlemlerinin mevcut durumunu içermelidir. Üçüncü olarak, kamu bulut sağlayıcılarının itibar ve güvenilirliklerini arttırmaları gerekir. Daha spesifik olarak bir açık/toplum bulutu mimarisi şunları desteklenmelidir:

- E-Devlet hizmetleri için çok kiracılı altyapıların kullanımı ile ilgili bir AB yönetmeliği,
- Kamu bulut sağlayıcının yeterliliğini tasdik etmek/değerlendirmek için bir çerçeve (Örneğin şeffaf denetim prosedürlerini sağlayan gönüllü bir sertifikasyon programı),
- Bulut hizmetlerini temin etmesi gereken tüm devlet organları için kamu ihale çerçevesi,
- Yurt dışı tedarik ile ilgili sorunlarla başa çıkmak için yasal bir çerçeve,

- Uygulama ve veri taşıma için standart prosedürlerin tanımı,
- Veri yerelliğini kontrol/izleme ve genel olarak veriyi ele almak için bir çerçeve.

Öneri 3: Kontrol kaybını azaltmak için bir çerçeve

Veri ve kaynak kontrol kaybı, kamu bulutu önündeki en önemli engellerden biri olarak dikkat çekmektedir. "Kontrol kaybı" sorunu sadece bir teknoloji meselesi olmayıp; aynı zamanda farkındalık, şeffaflık, hukuksal düzenleme, sağlayıcılar ve kamu müşterileri arasındaki sözleşmeler meselesidir. Örneğin bir kamu kurumu, sahibi oduğu veri ve uygulamalarını buluta aktardığında, bulut sağlayıcı prosedürlerindeki şeffaflık eksikliği (örneğin veri bozulması için standart prosedürler), ortak sözleşme hükümlerinin ve bir AB yönetmeliğinin olmaması sebepleriyle, bulut sağlayıcının verilerine erişme ve verilerini manipüle etme ihtimali nedeniyle endişe duyabilir. Kontrol kaybının bir başka yönü sağlayıcıya bağımlılık sorunudur. Örneğin sağlayıcının iflası durumunda, veri ve uygulamaların akıbeti hakkında endişeler ortaya çıkabilmektedir. Sağlayıcıya bağımlılığa ilişkin maliyet ve zaman kısıtlamaları olmadan, her zaman bir sağlayıcıdan başka bir bulut sağlayıcıya veri ve uygulamaları aktarmak mümkün olmalıdır. Bütün bu hükümlerin hizmet seviye anlaşmasında beyan edilmesi ve anlaşılması gerekmektedir.

Tedbirler: Bulut sağlayıcıları ve kamu müşterileri ile işbirliği içinde Avrupa Komisyonu ve Üye Ülkelerin yetkili makamları; yönetim, izleme ve denetim, sağlayıcı bağımlılığı ve veri işleme konularını yakından ele alarak, "kontrol kaybını" azaltmak için çalışma yapmalıdırlar. Bu konuda atılması gerekli adımlar şunlardır:

1- Kamu bulutundaki kamu hizmeti katmanları için bir izleme ve denetim çerçevesinin tanımı,

2- Veri işleme için standart prosedürlerin tanımı,

3- Veri ve hizmet aktarımı için standart prosedürlerin tanımı,

Öneri 4: Yerellik sorununu çözmek için bir düzenleyici çerçeve

Bulut sağlayıcıları genellikle farklı birçok ülkede bulunabilen kendi veri merkezlerinde verileri depolarlar. Ülke dışında veri ve kaynakları bulundurma olasılığı, genellikle veri gizliliği sorunları nedeniyle, kamu bulutunun benimsenmesi için bir engel olarak algılanmaktadır. Verinin konumu için düzenleyici çerçevenin tanımı, kamusal kullanıcıların bulut mimarisine itirazlarını azaltabilir ancak veri koruması için en kritik endişe verilerinin konumundan çok güvenliğinin sağlanmasıdır. Bunu elde etmek için, teknik çözümlerin (örneğin şifreleme kullanımı) uygun olduğu belirtilmiştir. Ancak, risk sadece teknik önlemlerin alınması ile ilgili değildir. Genellikle yerel yargı sadece kamu tarafından sahip olunan verilerin yurtdışında bulunmasını yasaklamaktadır. İkincisi, bu durum sadece veri konumundan ibaret olmayıp, aynı zamanda bulut sağlayıcının hangi yasal çerçeye girdiği ile de ilgilidir.

Ayrıca daha küçük ülkeler için, verilerin yurtdışında barındırılmasının engelleyici maliyetleri olduğu ve yine kendi veri ve yedekleme merkezlerini kurmanın da zor olacağı unutulmamalıdır. Düzenleyici çerçeve bunu dikkate almalı ve bunun üstesinden gelmek için çözümler sunmalıdır.

Tedbirler: Yeni bir çerçeve tanımı için, Avrupa Komisyonu ve Üye Ülkelerin yetkili makamlarının, bulut sağlayıcıları ve kamu müşterileri ile işbirliği içinde aşağıdaki konularda çalışmaları gerekmektedir:

1- Kamu kurumları ve bulut servis sağlayıcılarının konuyla ilgili mevcut AB mevzuatı hakkındaki farkındalılıklarını geliştirmek için gerekli önlemlerin tanımı,

2- Mevcut mevzuat ile uyumlu teknolojik çözümler geliştirilmesinin teşvik edilmesi,

3- Veri sahipliği ve veri gizliliği ile ilgili kamu kurumu gereksinimlerinin, eldeki verilerin türüne göre değerlendirilerek sınıflandırılması,

4- Veri ve kaynak mülkiyeti hakkında, dış kaynak kullanımı üzerine odaklanılarak mevcut AB mevzuatının iyileştirilmesi.

5- Dış kaynak kullanımına odaklanarak, veri gizliliği ile ilgili mevcut AB mevzuatının geliştirilmesi.

Öneri 5: AB ve ulusal hukuk ile uyumlu kamu bulutu çözümleri

Servis sağlayıcılar tarafından önerilen teknolojik çözümler hakkında kamu kurumlarının şüphelerinin yumuşatılması için, AB düzenlemeleri ve ülkeye özel mevzuatlara uyumlu sistemler ve hizmetlerin geliştirilmesini teşvik etmek için önlemler alınmalıdır.

Tedbirler: Bulut sağlayıcıları ile işbirliği içinde Avrupa Komisyonu ve Üye Ülkelerin yetkili makamları, kamu organları, standardizasyon kuruluşları ve Ar-Ge sektörü; AB ve ulusal mevzuatlara uygun teknolojik çözümler gelişmesini teşvik etmeye çalışmalıdır. Atılması gerekli adımlar şunlar olacaktır:

1- Her bir bulut çözümünün, ilgili mevzuat (ulusal ve / veya AB hukuku) ile uyumlu olduğunu, tasdik veya garanti eden bir akreditasyon çerçevesi (sertifikasyon) kurulması,

2- Yasal uyumlulukları kapsayacak şekilde standart sözleşmelerin tanımlanmasının teşvik edilmesi,

3- AB ve Üye Ülkelerin düzenlemelere ilişkin farkındalığının arttırılması,

4- AB devletleri için bulut konularında eğitimin teşvik edilmesi.

Öneri 6: Hizmet Seviye Anlaşması (SLA) için ortak bir çerçeve

Standart hizmet seviyesi anlaşmaları için ortak bir çerçevenin geliştirilmesi, kamu bulutlarının kurulumunu artırmak için bir önlem olacaktır. Bir hizmet seviyesi anlaşması çerçevesine sahip olmak suretiyle; sözleşmelerin tanımı ve kamu bulut çözümleri hakkındaki şüpheler gibi kamu kuruluşlarının yaşayacağı zorluklarla başa çıkılabilir. Bu çalışma, AB Bulut Stratejisinde başlatılmıştır ve ENISA tarafından desteklenmektedir.

Tedbirler:

1- Bulut sağlayıcıları tarafından kamu kuruluşlarına verilen güvence ve garantiler; güvenlik ve gizlilik iddialarını desteklemek için, belirli penetrasyon testleri içermeli ve ayrıca bağımsız üçüncü şahıslar tarafından yapılacak denetim faaliyetleri ile doğrulanmalı ve değerlendirilmelidir. Müşteriler denetimin tekrarından kaçınmak için, üçüncü parti denetçiler tarafından yapılan tasdik/yorumlardan yararlanabilirler.

2- Olaya müdahale ve raporlama yükümlülüğünün yerine getirilmesi ve olaylara sağlayıcıların derhal yanıt vermesi sağlanmalıdır. Kritik görünen ve hizmetlerin kullanılabilirliğini etkileyebilecek olayları, ilgili makamlar ve/veya kamu kullanıcılarına rapor etmek, saldırı ve hatalardan hızla kurtarmak amaçları içeren sözleşme şartları uygulanmalıdır.

3- Olaya müdahale ve raporlama, özellikle hizmet türü veya veri hassasiyeti açısından belli bir düzeyde kritikliğe sahip kamu hizmetleri için gereklidir. Bu durumlarda, tepki ve raporlama zaman çizelgeleri açısından hizmet seviye anlaşmalarını ayırmak yararlı olacaktır.

4- Hizmet düzeyi kısıtlamalarının ihlali durumunda kesilecek cezalar sözleşmeye dâhil edilmelidir. Bu konuda benzer bir hizmet sözleşmesi veya benzeri standardize sınıflandırmalara karşı geçmiş ihlallerle ilgili, kullanıcıları bilgilendirmek için kullanılacak bir itibar (not) sisteminin oluşturulması dikkate değer görünmektedir.

Öneri 7: Kamu bulutu için güvenlik önlemleri

Hizmetlerin ve sağlayıcıların güvenlik sertifikasyonu için, standart yaklaşım ve yöntemler tanımlamak bulut mimarilerinin güvenilir şekilde kullanılabilmesi için önemlidir. Kamu kurumlarının güvenliğini sağlamak için, bulut sağlayıcıların sertifika yoluyla uyum sağlamak zorunda olduğu kapsamlılık düzeylerinden oluşan ve her bir güvenlik düzeyinde açıkça gereksinimleri tanımlayan bir model geliştirilmesi gerekmektedir. Bulut hizmetlerinin akreditasyon modeli ancak bu işe adanmış merkezi

bir idare tarafından uygulanabilir. Kamu kullanıcıları ve sağlayıcıları, kamu hizmetleri için talep edilen ve sağlanan güvenlik seviyesini seçmek konusunda özgür olmalı ve ilgili birimlere en etkili ve ucuz mali çözümler içinden en iyisini uygulama seçeneği bırakılmalıdır. Kamu bulutu kurulumuna odaklanmış spesifik bir dizi güvenlik önlemi, bulut tedarik zincirinde güvenilirliği artırmanın bir yolu olacaktır.

Tedbirler: Kamu bulutu hizmetlerinde güvenliğin ve bilginin korunmasının artırılması için önerilen eylemler:

1- Hizmet satın alma öncesi ön değerlendirme sürecini desteklemek,

2- Kamu bulutlarına odaklanmış bir dizi temel güvenlik önlemi oluşturmak (Bu önlemler güvenlik yönetimi, kimlik yönetimi, veri yedekleme hizmetleri ve ulaşılabilirlik vb gibi alanlar içermelidir.),

3-Sofistike/gelişmiş bir model sunmak için her alanda risk etki düzeylerini içeren; bilgi güvenliği önlemlerinin denetim (ve/veya sertifikasyon) çerçevesini etkinleştirmek;

4- Güvenlik etiketleme sistemlerini teşvik etmek.

Öneri 8: Sertifikasyon çerçevesi

Kamu yönetimi çerçevesi dikkate alındığında, sorunun kamu kurumlarında sertifikaların yaygın olmaması olduğu anlaşılır. Kamu kurumları bir dış denetçi tarafından onaylanmaya gerek duymadan, standartlara uyumlu olmayı tercih ederler. Şu anda AB Bulut Stratejisi kapsamında Avrupa Komisyonu, bulutta sertifikaları destekleyen faaliyetleri başlatmış ve daha da önemlisi tüm sağlayıcıların akredite olması için bir meta çerçevesi oluşturmaktadır. ENISA, bu eylemin sorumlusu olarak seçilen sanayi grubunun bir parçası olup, tamamen Avrupa Komisyonu'nu destekler. Bu çalışma, AB Bulut Stratejisinde başlatılmış olup ve ENISA tarafından desteklenmektedir.

Tedbirler:

1- Kamu bulutu platformunun ve hizmetlerinin sertifikasyonuna yönelik bir yaklaşım tartışmalı ve zor bir süreçtir. Hedefe ulaşmak için ana sürücü, bu yükümlülüğü AB düzenleyici çerçevesine veya bir Avrupa gönüllü sertifika düzenine dâhil etmek olabilir.

2- Küresel kalkınma ve sanayi kaynaklı standartlar ve ayrıca diğer ülkelerdeki kamu gereksinimleri keşfedilmelidir.

3- Ulusal bir "önceden denenmiş bulut ürünleri/uygulamaları hizmet katalogları" oluşturulmasını desteklemek gereklidir. Bu yaklaşım "Bir kere emin ol defalarca kur" modelini uygulayarak hizmetin maliyetini azaltır.

4- Bu eylem, bulut hizmetlerini kamu sektörüne sunmak isteyen tüm sağlayıcılar için bir Avrupa akreditasyon sistemi oluşturarak, önceki güvenlik önlemi önerileri ile birleştirilebilir. Bilgi güvenliği alanında, alan başına güvenlik kontrolleri de içeren ve sofistike seviyeleri sınıflandırılan bir meta çerçeve, iyi bir başlangıç noktasıdır.

Öneri 9: Kamu bulutu güvenliği konusunda araştırmaları teşvik

Kamu gereksinimleri ile uyumlu bulut teknolojilerinin gelişimini desteklemek için, mevcut araştırma programlarından yararlanarak, kamu bulutu araştırmalarını teşvik etmek önemlidir. Araştırmalar kamu hizmetleri için bulut çözümlerinin risk etki düzeyini yükseltmeye yönlenmelidir.

Avrupa Komisyonu ve Üye Ülkelerin Ar-Ge yetkili makamları ve akademik işbirliğiyle; bulut sağlayıcıları, mevcut ve gelecekteki ulusal ve Avrupa araştırma programlarını desteklemeli (örneğin Horizon 2020) ve kamuda bulut bilişimin güvenlik yönleri üzerine kendi çalışma konularını araştırma programlarına dâhil etmelidir. Bu araştırma konularından bazıları şunlardır: Bulut servis kullanım süresi yönetimi, bulut tedarik zinciri kontrolü, olay yönetimi, siber risk analizi, siber tehdit modelleme, şifreleme, veri koruması, bulut gizlilik ve güvenlik ölçümü, gizlilik seviyesi anlaşması, veri koruma için hesap verebilirlik ve şeffaflık ve bulut sistemlerinde bilgi güvenliği.

Tedbirler: Avrupa Komisyonu ve Üye Ülkelerin yetkili makamları; bulut sağlayıcıları, kamu müşterileri, Ar-Ge sektörü ve akademik işbirliği ile aşağıdaki eylemleri üstlenmelidir:

1- Farklı araştırma hedefleri için önceliklerini oluşturmak,

2- AB ve ulusal düzeyde mevcut güvenlik araştırma programları ile iletişim kurmak (Horizon 2020 gibi),

3- Uygun kurum ve kuruluşlarla (Örneğin Çerçeve Program Komitesi ve Danışma Grupları, Teknoloji Platformları, vb) uygun bir çalışma programı tanımlamak için birlikte çalışmak.

Öneri 10: Veri gizliliğinin icrası

Veri koruma, kamu bulutları içerisinde işlenen bilgilerin hassasiyeti nedeniyle önemli bir konudur. Avrupa Komisyonu ve Üye Ülkelerin bulut hizmetlerinin, AB veri koruma yasalarına uyumlu olmasının sağlanması gerekir. Bulut hizmetlerinde gizliliği garanti etmek için, bulut sağlayıcı tarafından şifreleme ve kullanıcılar tarafından kimliği doğrulanmış erişim basit bir çözüm gibi görünmektedir. Ancak bulut hizmetlerinde kriptografik çözümlerin uygulanması hala düşük gelişmişlik seviyesindedir.

Tedbirler: Veri koruma icra teknikleri temel bir mesele haline gelmiş olup, aşağıdaki gibi kontrollü ve kriptografik teknikler çözümün bir kısmını temin edebilir:

1- Kuruluş tarafından kişisel bilgilerin yönetimi hakkında, yurtdışı kullanıcıların muhtemel dipnotları ile elde edilen bilgileri de içeren ve açık bir şekilde ifade edilen güncel politikalar dikkate alınmalıdır.

2- Servis olarak Altyapı (IaaS) ve Servis olarak Platform (PaaS) modellerinin yanı sıra özel bulutlarda kriptografi de gizlilik garantisi vermez. Özel bulutta veri güvenliği; şifreleme teknikleri yerine, erişim kontrolü gibi diğer yollarla sağlanmalıdır.

3- Servis olarak Yazılım (SaaS) hizmetlerinin sağlanmasında, sağlayıcının müşteri ile sözleşmesinde kriptografik çözümler istek üzerine değil, ön tanımlı olarak bulunmalıdır.

4- Gizlilik Servis olarak Altyapı (IaaS) ve Servis olarak Platform (PaaS) için açıkça gerekli olduğundan, sağlayıcıların sunduğu şifreleme işlevlerine alternatif çözümler de dikkate alınmalıdır. Bu çözümler, bu servis modelleri üzerindeki kontrolü etkinleştiren ve şifreleme işlemlerinin uygulanmasını onaylayan bir üçüncü parti tarafından (tercihen bir kamu departmanı veya güvenilen bir güvenlik servis sağlayıcı) barındırılan ve yönetilen, buluta depolamadan önceki kamu hizmetlerinin şifreli verilerini veya şifreleme hizmetlerinin kullanımını (örneğin anahtar yönetimi sunucuları, sunucular için erişim ilkesi gibi) içerebilir (Decker, 2012).

3. BULUT BİLİŞİM RİSK ANALİZİ

2000'li yılların başlarından bu yana, özellikle gelişmiş ve gelişmekte olan ülkelerde özel sektör kuruluşlarının yanısıra kamu kurum ve kuruluşları, iş verimliliklerini artırmak (daha az personel marifetiyle vatandaşlarına daha etkin hizmet sunabilmek), maliyetlerini azaltmak, stratejik karar verme süreçlerini kolaylaştırmak ve hizmetlerine vatandaşların daha kolay erişebilmesini mümkün kılmak gibi birçok sebeple; en yeni ve güncel bilişim teknolojilerini temin etme ve kullanma yarışına girmişlerdir. Bu bağlamda yeni ve güncel hizmet modeli sunan bulut bilişim konusunda ülkeler, özellikle 2010'lu yılların başlarından bu yana proje ve stratejiler geliştirmekte ve geleneksel bilişim mimarisi üzerinden vatandaşa sundukları hizmet ve uygulamalarını hızla bulut bilişim mimarisine taşımaktadırlar. Bulut bilişim mimarileri kullanıcılarına sağladığı sayısız faydanın yanında birtakım risk, tehdit ve zafiyetler de barındırmaktadır. Bu risklerin bazıları hali hazırda kullanılan geleneksel bilişim mimarileri ile ortak riskler olsa da, bulut bilişimin de kendine has riskleri mevcuttur. Bu risklerin belirlenmesi, değerlendirilmesi, analizi ve yönetimi; uzun vadede bu risklerden kaynaklanacak hizmet kalitesinin ve sürekliliğinin bozulması, zaman kayıpları ve ekonomik kayıplar ve ayrıca bunlara bağlı olarak kuruluşun itibarı ve güvenilirliği ile ilgili kamuoyunda oluşabilecek olumsuz intibanın önlenmesi açısından önemlidir. Bu risklerin kurum ve kuruluşların yararına yönetilebilmesi için belli başlı uluslararası standartlar belirlenmiştir.

Kuruluşların kullandıkları bilgi sistemlerindeki risklerin yönetilmesi ile ilgili, ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı gerekli faaliyetleri ortaya koyan bir standarttır. Bu standart kuruluşların, bilgi risklerini tanımladığı, analiz ettiği ve adreslediği kapsayıcı bir yönetim çerçevesidir. Standart güvenlik ile ilgili düzenlemelerin; güvenlik tehditleri, açıkları ve iş etkisinde meydana gelen değişikliklere ayak uydurmak için ayarlanmasını sağlar.

ISO/IEC 27005, Bilgi Güvenliği Risk Yönetim Standardıdır. Bilgi güvenliği risk yönetimi için kurallar sağlar ve ISO/IEC 27001 standardında belirtilen genel kavramları destekler. Bu standart kurumların ihtiyaçları doğrultusunda bir risk yönetim metodolojisi

geliştirmesi gerektiğini ifade eder ve mevcut risk yönetim metodojilerine ilişkin örnekler verir. Bu doğrultuda risk işleme, riskin kabulü, risk iletişimi, risk izleme ve risk gözden geçirme konularında, risk değerlendirme tavsiyeleri de içeren, bilgi güvenliği risk yönetimi kılavuzluğu sağlamaktadır. Standart risk yönetimi yaklaşımına dayalı bilgi güvenliğinin, tatmin edici şekilde uygulanmasına yardımcı olmak için tasarlanmıştır.

Yine TS ISO 31000 Risk Yönetimi Standardı, kurum veya kuruluşların genel idaresi, stratejisi ve planlaması, yönetimi, rapor verme süreçleri, politikaları, değerleri ve kültürü doğrultusunda; risk yönetimi ile ilgili süreci bütünleştirmek amaçlı bir çerçeve geliştirmesine, uygulamasına ve sürekli olarak iyileştirmesine yöneliktir. Bu standart kuruluşların, herhangi bir karakterdeki riski sistematik, şeffaf ve güvenilir bir şekilde, kapsam ve içerik dâhilinde yönetmesi için prensipleri ve genel esasları sağlar.

Ayrıca Türk Standardları Enstitüsü bünyesinde faaliyet gösteren Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubu tarafından hazırlan, Bulut Bilişim Güvenlik ve Kullanım Standardı Taslağı'nda; Bulut Bilişim Kontrol Listesinin Risk Yönetimi başlıklı 8. bölümünde:

- Kuruluşların, riski belirli bir seviyede tutmak için kurumsal risk yönetimini geliştirmesi ve sürdürmesinin,
- Asgari yıllık olarak veya planlanan aralıklarla resmi (formal) risk değerlendirme işleminin yürütülmesi ve bu esnada risklerin gerçekleşme olasılığı ve etkisinin incelenmesi,
- Risklerin kabul edilebilir bir seviyeye indirilmesi ve bu kabul seviyelerinin yönetimin onayına sunulması,
- Risk değerlendirme sonuçlarının; güvenlik politikaları, prosedürler, standartlar ve kontrollerdeki değişiklikleri de kapsaması,
- Kuruluşun bilgi sistemlerine ve verilerine üçüncü parti erişimle ilgili risklerin tanımlanması, değerlendirilmesi ve önceliklendirilmesinin ardından, koordineli

bir şekilde yetkisiz ve uygun olmayan erişimin etkisini düşürecek tedbirler alınması;

gerektiği belirtilmiştir (TSE, 2014). Bu sebeplerle, kamu kurum ve kuruluşlarında bulut bilişim mimarisi kullanımının yaratacağı risklerin analiz edilmesi amacıyla bu bölümde risk analizi çalışması yapılacaktır.

3.1. Risk, Risk Analizi ve Risk Yönetimi

Risk, belirli bir tehdidin, sistemin belirli bir zayıflığından faydalanarak sisteme zarar verme ihtimalidir. Karşı önlemleri almadan önce büyük olan risk, karşı önlemleri aldıktan sonra azalır. Karşı önlemler alınmadan önce sistemde mevcut olan riske taban riski, karşı önlemler alındıktan sonra sistemde mevcut olan riske ise artık risk denilmektedir (TS ISO/IEC 27000:2014).

Risk analizi, TS ISO/IEC 27001:2005 standardında, kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmıştır. Risk analizi süreci kapsam belirlenmesi ile başlar. Belirlenen kapsamda bulunan varlıklar belirlendikten sonra; tehditler, zafiyetler ve mevcut riskler belirlenir. Daha sonra olasılık değerlendirmesi ve etki analizi gerçekleştirilir. Son olarak bulunan riskler derecelendirilerek dokümante edilir (Eskiyörük, 2007). Bu tez çalışmasında bu standardın belirlendiği yöntemler doğrultusunda bir risk analizi çalışması yapılacaktır.

Risk yönetimi; risklerin tanımlanması, analiz edilmesi, değerlendirilmesi, denetlenmesi ve kaçınılması, minimizasyonu ve kabul edilemeyecek risklerin ortadan kaldırılması süreçlerini içeren bir stratejik faaliyettir. Burada kuruluş gelecekte meydana gelebilecek olayları doğru yönetebilmek maksadıyla; süreç içinde risk varsayımı, riskten kaçınma, risk tutma, risk transferi veya başka bir strateji kullanabilir.

Risk yönetiminde öncelikle potansiyel risklerin belirlenmesi gerekmektedir. Risk belirlemede risk kategorileri bazında bir çalışma yapmak, önemli risk alanlarının unutulmasını engeller. Örneğin, her kuruluş girdileri, üretim süreçleri, piyasa şartları,

finansal piyasalar, hukuka aykırılık, kanunlarda ve denetim kurumlarındaki değişiklikler ve vergi konularındaki risklerini belirlemelidir.

İkinci adımda ise tanımlanan risklerin gerçekleşme olasılıkları ve gerçekleşmeleri durumunda kuruma yükleyeceği maliyetler (etkileri) ile ilgili değerlendirmelerin yapılması gerekmektedir. Bu değerlendirme ışığında riskler gruplandırılarak alınacak tedbirler belirlenir. Örneğin, potansiyel etkisi yüksek ancak gerçekleşme olasılığı düşük risklerin sigortalanması veya kiralama gibi farklı finansman yöntemleriyle yönetilmesi sağlanırken, potansiyel etkisi düşük ve gerçekleşme olasılığı yüksek risklerin azaltılması için yatırım yapılması tercih edilebilir.

3.2. Bulut Bilişimde Varlıkların Belirlenmesi ve Modellenmesi

Bir varlık, kuruluşun iş operasyonları ve sürekliliği için değerli olan her şeydir. Bu nedenle kuruluşun iş sürekliliğini sağlamak için varlıklarını koruması gerekmektedir. Risk yönetimi çözümünde, kuruluşun kendi önem verdiği varlıklarının tam listesi yer almalıdır. Varlık envanteri olarak isimlendirilen bu liste, risk analizi süreci için temel bir girdidir. Burada varlık envanterinin güncel ve uygun bir şekilde gruplandırılmış varlıklardan oluşturulması, risk değerlendirme çıktıklarının doğruluğu açısından kritik bir konudur. Risk yönetiminin temel yöntemlerinden biri zafiyetleri, tehditleri ve varlıkları birbirleri ile ilişkilendirmek ve varlıkların değerine göre riskin gerçekleşemesinin kuruluşa olan etkisini hesaplayıp; risk değerini ve bulunan bu risk değerlerine göre riskleri sıralayıp yönetmektir.

3.2.1. Bulut Bilişimde Varlıkların Belirlenmesi

Bulut bilişimde en değerli ve önemli varlık türlerinden biri bilgidir ve bu varlıklar güçlü biçimde korunmalıdır. Bilgi, veri tabanları veya dosyalar formunda olabilir. Buna ek olarak, bilgiyi saklayan veya işleyen süreçler ile bulut güvenliği konusunda etkisi olan varlık benzeri süreçler korunmalıdır.

Belirlenen varlıklar için doğru korumayı bulmak için, kuruluşun hizmetleri açısından değerlerini belirlemek önemlidir. Varlık değerlerini ifade etmenin bir yolu; bu

varlık ile ilgili yaşanabilecek ifşa, değişiklik, kullanılamazlık veya imha gibi istenmeyen olayların, ilgili kuruluşun faaliyetlerine etkilerini belirlemektedir. Bu etkiler; kuruluşun gelir, pazar payı, piyasa değeri veya itibar kaybı gibi, faaliyetlerine yönelik mali olumsuzluklar olabileceği gibi; verimlilik düşüşü, çalışan güven kaybı, iş taahhütleri ve iç operasyonlarının aksaması gibi iş sürecine yönelik de olabilirler.

Bulut bilişimde meydana gelebilecek tehdit ve zafiyetlerin yarattığı risklerden etkilenebilecek varlıklar, büyük oranda geleneksel bilişim sistemlerindekilerle benzerlik göstermektedir. Ancak bulut bilişim mimarisininde bu varlıklar üzerinde oluşacak risk etkileri, geleneksel mimariyle aralarındaki uygulama farklılıkları nedeniyle önemli değişiklikler göstermektedir.

Bulut bilişimin karşı karşıya kaldığı operasyonel, teknik veya yasal risklerden etkilenebilecek varlıklarından büyük bir kısmı bilgi ve veri varlıklarıdır. Bu varlıklara kişisel veriler, kişisel hassas veriler, insan kaynağı verileri, kimlik bilgileri, operayonel ve güvenlik logları, kullanıcı dizini ve yedekleme ve arşiv verileridir.

Bir diğer varlık kategorisi olarak yazılım varlıkları verilebilir. Bu varlıklara; bulut hizmeti yönetim arabirimi, yönetim arayüzü API'leri, sanal makineler, erişim kontrol, doğrulama, yetkilendirme yazılımları, sağlayıcı uygulamaları, ağ ve haberleşme yazılımları ve müşteri uygulamaları verilebilir.

Bir başka varlık türü ise fiziksel varlıklardır ve bu varlıklara fiziksel donanım (sunucu, depolama ünitesi, ağ ve haberleşme donanımı vb.) ve fiziksel binalar örnek olarak verilebilir.

Bulut bilişimde meydana gelebilecek problemlerden ciddi şekilde etkilenebilecek, insan davranışıyla ilgili soyut varlıklar da bulunmaktadır. Kuruluş itibarı, müşteri güveni, çalışan sadakati ve deneyimi bu varlılara örnek olarak verilebilir.

Bunların yanında müşteri hizmet sunumu, sağlayıcı hizmet sunumu, fikri mülkiyet hakları ve belgelendirme gibi bulut hizmetlerinde meydana gelebilecek aksamalardan etkilenebilecek diğer varlıklar da mevcuttur.

3.2.2. Bulut Bilişimde Varlıkların Modellenmesi

Bulut bilişim mimarisi ile ilgili tehdit ve zafiyetlerin yarattığı risklerin, yukarıda belirtilen varlıklar üzerindeki etkilerini belirleyebilmek için, bu varlıkların sahiplerinin ve değerlerinin belirlenmesi gerekmektedir. Aşağıdaki tabloda bulut bilişim hizmet modelinden etkilenen varlıkların sahiplik ve değer durumları belirlenmiştir. Burada bulut sağlayıcı, müşterisi veya her ikisine birden ait olan varlıkların (müşteri kiralama yoluyla sağlayıcı varlıkları üzerinde sahiplik hakkı elde edebilir) sahipleri ve beş kademeli olarak değerlendirilen (düşük ve çok düşük varlık değeri atanan varlık bulunmamaktadır) varlık değerleri belirtilmektedir.

Varlık Adı Ve Kodu	**Varlık Sahibi**	**Varlık Değeri**
V.1- Kişisel veriler	Sağlayıcı ve Bulut müşterisi	Yüksek
V.2- Kişisel hassas veriler	Sağlayıcı ve Bulut müşterisi	Çok Yüksek
V.3- İnsan kaynağı verileri	Bulut müşterisi	Yüksek
V.4- Kimlik bilgileri	Bulut müşterisi	Çok Yüksek
V.5- Operayonel ve güvenlik	Sağlayıcı ve Bulut	Orta

logları	müşterisi	
V.6- Kullanıcı dizini	Bulut müşterisi	Yüksek
V.7- Yedekleme ve arşiv verileri	Sağlayıcı ve Bulut müşterisi	Orta
V.8- Bulut hizmeti yönetim arabirimi	Sağlayıcı ve Bulut müşterisi	Çok Yüksek
V.9- Yönetim arayüzü API'leri	Sağlayıcı ve Bulut müşterisi	Orta
V.10- Sanal makineler	Sağlayıcı ve Bulut müşterisi	Yüksek
V.11- Erişim kontrol, doğrulama ve yetkilendirme yazılımları	Sağlayıcı ve Bulut müşterisi	Yüksek
V.12- Sağlayıcı uygulamaları	Sağlayıcı ve Bulut müşterisi	Yüksek
V.13- Müşteri uygulamaları	Bulut müşterisi	Yüksek
V.14- Ağ ve haberleşme yazılımları	Sağlayıcı ve Bulut müşterisi	Orta

V.15- Fiziksel donanım (istemci, sunucu, depolama ünitesi, ağ ve haberleşme donanımı vb.)	Sağlayıcı ve Bulut müşterisi	Orta
V.16- Fiziksel binalar	Sağlayıcı ve Bulut müşterisi	Yüksek
V.17- Kuruluş itibari	Bulut müşterisi	Çok Yüksek
V.18- Müşteri güveni	Bulut müşterisi	Çok Yüksek
V.19- Çalışan sadakati ve deneyimi	Bulut müşterisi	Yüksek
V.20- Müşteri hizmet sunumu	Bulut müşterisi	Yüksek
V.21- Sağlayıcı hizmet sunumu	Sağlayıcı ve Bulut müşterisi	Çok Yüksek
V.22- Fikri mülkiyet hakları	Bulut müşterisi	Yüksek
V.23- Belgelendirme	Sağlayıcı ve Bulut müşterisi	Yüksek
V.24- İş taahhütleri	Sağlayıcı ve Bulut müşterisi	Yüksek

Tablo 3.1: Bulut Bilişim Varlık Listesi

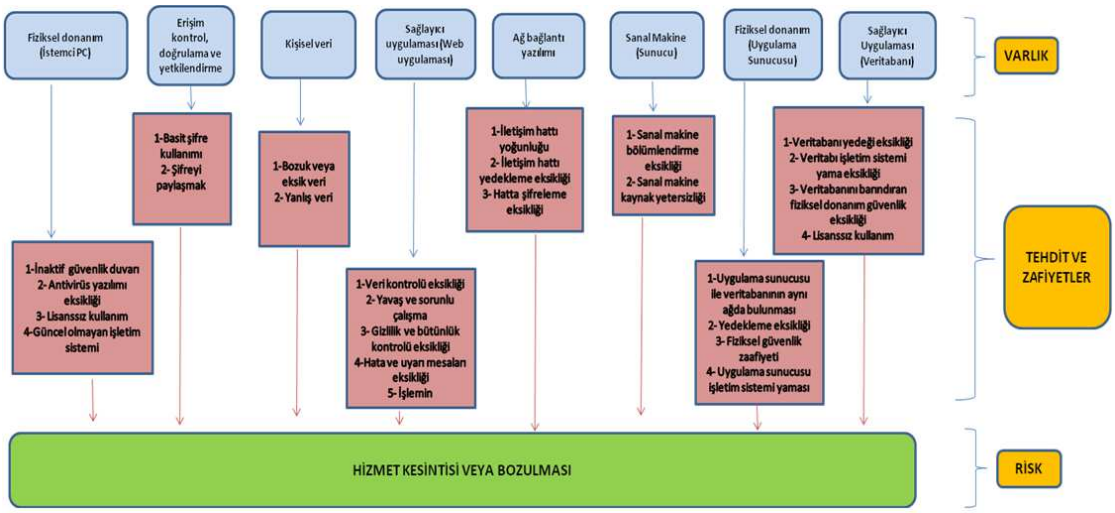
Tabloda görüleceği üzere, kuruluş itibari ve müşteri güveni varlıklarının çok yüksek varlık değerine sahip olduğu belirtilmiştir. Bu durumun sebebi, bu varlıkların uzun yıllar boyunca yapılan başarılı hizmetler sonucu elde edilen ve bir kez kaybedildiğinde, geriye kazanılması güç olan olgular olmalarıdır. Yine bulut hizmeti yönetim arabirimi ve sağlayıcı hizmet sunumu varlıkları, ilgili bulut altyapısındaki bütün müşterileri etkileme potansiyeline sahip olmaları sebebiyle; çok yüksek varlık değerine haiz kabul edilmişlerdir. Aynı şekilde kişisel hassas veriler ve kimlik bilgileri, kişiye özel ve kötü amaçlar için kullanılabilme riski yüksek olan veriler olup, ifşa veya kayıpları büyük zararlar yaratabileceğinden çok yüksek varlık değerine atanmışlardır.

Yedekleme ve arşiv verileri, operayonel ve güvenlik logları, yönetim arayüzü API'leri, ağ ve haberleşme yazılımları, fiziksel donanım (sunucu, depolama ünitesi, ağ ve haberleşme donanımı vb.) gibi varlıklara orta derece varlık değeri verilmesinin sebebi; bu varlıkların bir şekilde yerine konabilecek ve kaybolmaları veya zarar görmeleri durumunda bulut hizmetini belli bir müşteri veya müşteri grubu için kısa vadeli olarak kesintiye uğratacak varlıklar olmalarıdır.

Belirlenen diğer varlıklara ise yüksek seviyeli varlık değeri atanmıştır. Birçok farklı kategorideki bu varlıklar, genel olarak zarar görmesi veya bozulması durumunda bir şekilde yerine konabilecek fakat ciddi düzeltme maliyeti gereksinimi yaratacak varlıklardır.

Aşağıdaki tabloda, bulut bilişim mimarilerinde belirlenen bazı varlıkları etkileyebilecek, tehdit, zafiyet ve risklerle ilişkilerinin modellendiği bir akış diyagramına yer verilmiştir. Bu akış diyagramında, muhtelif bir bulut uygulamasının kullanımı sırasında, kullanım için gerekli olan varlıklar arasındaki işlem sıralaması ve bu işlemler sırasında ilgili varlığın maruz kalabileceği tehdit ve zafiyetlere örnekler verilmiştir. Bu tehdit ve zafiyetlerden etkilenen varlıkların herhangi birinin bozulması, yetersiz işlev göstermesi veya tamamen devre dışı kalması sebebiyle; aşağıda belirtilen hizmet kesintisi veya bozulması riski meydana gelebilecektir. Bu modelleme birçok varlığın ilgili risk üzerindeki etkisini gösterme kabiliyeti taşıdığından, ilgili riskin oluşmasını

etkileyecek tehdit ve zafiyetlerin gözden kaçırılması ihtimalini düşürmektedir. İlgili riskin oluşmasını engellemek için, akış diyagramındaki iş sürecinin her aşamasında, varlıkları etkileyen tehditleri ve bu varlıklardaki zafiyetleri engellemek gereklidir. Burada belirtilen varlıkların her birinin varlık değeri, oluşabilecek risklerin risk etki değerleriyle doğru orantılıdır. Aşağıdaki tablo, belirtilen varlıklara ait diğer tehdit ve zafiyetler ile birlikte; farklı diğer varlıkların eklenmesiyle zenginleştirilebilir. Bulut bilişimdeki her bir risk için benzer akış diyagramları oluştrmak mümkündür.



Tablo 3.2: Bulut Bilişim Varlıkları Süreç Modellenmesi

3.3. Bulut Bilişimde Tehdit ve Zafiyetler

3.3.1. Bulut Bilişime Özel Tehdit ve Zafiyetler

Bulut bilişim teknolojileri, 24/7 kullanılabilirlik ve esneklik gibi özellikler sunarken; ölçek artışının ve sistemleri canlı ve dinamik tutma zorunluluğunun sebep olduğu sorunlar nedeniyle, tehdit ve zafiyetlerin yeni bir boyutuyla karşı karşıya kalmaktadırlar. Bu sebeple ağ, depolama ve işlemci sistemleri ile ilgili mevcut tehdit ve zafiyetlerin yanında; bulut bilişimin ortaya çıkardığı yeni sorun ve farklı güvenlik açığı konularında araştırma yapmak ve belirlenenleri kuruluşların risk yönetim sürecine eklemek, bulut toplumunun ve endüstrisinin yanında müşteri kuruluşların da yararına olacaktır. Bulut sistemlerinde görülen zaafiyet ve tehditlerin birçoğu arasında, ilgili

bulut hizmetinin servis modeli (IaaS, PaaS, SaaS) arkasındaki fiziksel altyapı ve yönetim süreçleri gibi farklı bileşenleri yoluyla birbirine bağımlılık ilişkisi olup; birçok zafiyet ve tehdit birleşerek bulut bilişim hizmetleri ile ilgili riskler ortaya çıkarmaktadır. Bulut bilişim teknolojilerinde ortaya çıkan riskleri belirlemeden önce, bu risklere sebep olan tehdit ve zafiyetlerin belirlenmesi ve belirlenen risklerin ilgili tehdit ve zafiyetlerle eşleştirilerek profilinin oluşturulması, risk yönetim sürecinin temel yöntemlerinden biridir. Aşağıda bulut bilişim teknolojileriyle ilgili belli başlı tehdit ve zafiyetlere kısa açıklamalarıyla birlikte yer verilmektedir.

T.1- Hipervizörle İlgili Tehditler: Hipervizörler, fiziksel kaynakları ve bunun üstünde çalışan sanal makineleri tamamen kontrol ettiğinden bu tabaka ile ilgili güvenlik prosedürleri çok önemlidir. Hipervizörün kötüye kullanılması, her sanal makinenin kötüye kullanılması anlamına gelir. Bir hipervizördeki güvenlik açığını kullanarak yapılan en tipik saldırı çeşitlerinden biri sanal makine sızıntısıdır. Bu saldırıda saldırgan, sanal makine içinde çalışan bir işletim sistemi vasıtasıyla, hipervizörle ile doğrudan etkileşim sağlayan bir kod çalıştırır. Böyle bir kötüye kullanma, saldırganın ana işletim sistemine ve bu ana bilgisayarda çalışan diğer tüm sanal makinelere erişimine izin verebilir. Çok fazla yaşanan bir olay olmamasına rağmen sanal makine sızıntısı, sanal makine güvenliği için en ciddi tehdit olarak kabul edilir. Diğer bir tehdit olan sanal makine sekmesi, saldırganların bir sanal sunucudan diğerine hareket etmesine ve hatta fiziksel donanıma yönetici erişimi sağlamasına izin verir. Burada saldırgan önce bir sanal makineyi ele geçirir ve daha sonra hipervizörün güvenlik açıklarından faydalanıp onun yönettiği tüm sanal makineleri kontrolü altına alır.

T.2- Kaynak İzolasyon Eksikliği: Sanallaştırma teknolojilerinde bir müşteri tarafından gerçekleştirilen kaynak kullanımı, başka bir müşterinin kaynak kullanımını etkileyebilir. Servis olarak Altyapı (IaaS) bulut bilişim altyapıları çoğunlukla, fiziksel kaynakların birden fazla sanal makine ve birden fazla müşteri tarafından paylaşıldığı mimari tasarımlar sunarlar. Hipervizör güvenlik modelindeki açıklar, bu paylaşılan kaynaklara yetkisiz erişime yol açabilir. Örneğin, iki ayrı kullanıcıya ait sanal makinelerin sanal sabit diskleri, bir veri depolama ağı içinde paylaşılan aynı Mantıksal Birim Numarası'na

kaydedilirler. Kullanıcıların birinin sanal makinesiyle, diğer kullanıcının sanal sabit sürücüsünü eşleştirmesi mümkündür ve bu yolla içindeki verileri görebilir ve kullanabilir. Ayrıca bulut haritacılığı, müşterek ikamet ve çapraz yan kanal saldırısı açıkları üzerine kontrollerin eksikliği, kaynak izolasyonu için ciddi riskler oluşturabilir.

T.3- İletişim Şifreleme Tehditleri: Bu tehditlere örnek olarak MITM (aradaki adam saldırısı veya ortadaki adam saldırısı) verilebilir. Bu saldırıda saldırgan bir network üzerindeki kurban bir bilgisayar ile yönlendirici, switch, modem veya sunucu gibi diğer ağ araçları arasına girerek; verileri yakalama ve şifrelenmemiş verileri görebilme ilkesine dayanan bir saldırı gerçekleştirir. Bu saldırılar zayıf kimlik doğrulama, kendinden imzalı sertifika kabulü vb. açıklar yoluyla, aktarılan veriyi okuma prensibine dayanırlar.

T.4- Anahtar Oluşturma Tehditleri: Eğer bir sanal makine üzerinde anahtar belirlemeye yönelik rastgele sayılar oluşturmak için kullanılan işlem kaynakları benzer ise, bir saldırganın diğer sanal makinelerde üretilen şifreleme anahtarlarını tahmin etmesi mümkün olabilir. Bu çözülmesi zor bir sorun değildir, ancak sistem tasarımı sırasında dikkate alınmazsa önemli sonuçlar doğurabilir.

T.5- İç Ağda Tarama İşlemi: Aynı sağlayıcının hizmetlerinden faydalanan bulut müşterilerinden biri, iç ağ içindeki diğer müşterilere port taramaları ve diğer testler yapabilirler. Bu durum diğer müşterilerin veri ve uygulamaları için önemli bir tehdit oluşturur.

T.6- Müşterek İkamet Taramaları: Bulut mimarilerini tehdit eden yan kanal saldırıları, sistem algoritmalarındaki teorik zayıflıklar yerine, fiziksel şifreleme uygulanmasından elde edilen bilgilere dayanmaktadır. Örneğin sistem bilgisi, güç tüketimi, elektromanyetik sızıntılar ve hatta ses zamanlaması sistemi kırmak için kullanılabilir bir bilgi kaynağı sağlayabilir (Kocher, 1996). Kaynak izolasyon eksikliğinden faydalanan bu saldırılar, saldırganların hangi kaynağın hangi müşteri tarafından paylaşıldığını belirlemesine imkân sağlar.

T.7- Bulut Harici Sözleşme Kaynaklı Sorumluluklar: Bulut müşterileri genellikle hizmet seviye anlaşmasında kendilerine verilen sorumlulukların farkında değildir. Arşiv şifreleme gibi açıkça iki taraf arasındaki anlaşma hükümlerinde belirtilen ve bulut sağlayıcının böyle bir sorumluluk üstlenmediği konularda bile, sorumluluklar konusunda yanlış ilişkilendirmeye doğru bir eğilim bulunmaktadır.

T.8- Belgelendirme Programlarının Bulut Altyapısına Adapte Olmaması: Bu tehdit buluta özel herhangi bir kontrol veya denetimin yokluğunda ortaya çıkar ve bu durum güvenlik açıklarının gözden kaçırılmasını muhtemel hale getirmektedir.

Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri: Kimlik doğrulama, yetkilendirme ve kullanıcı hesabı ile ilgili hatalı kurulmuş bir sistem; kaynaklara ve ayrıcalıklara yetkisiz erişimi kolaylaştırır, kaynakların yanlış şekilde kullanılmasına yol açar ve genel olarak güvenlik olaylarını izlemeyi imkânsız hale getirir. Bu tehditlere başlıca, bulut erişim kimlik bilgilerinin müşteri tarafından güvensiz şekilde saklanması, yetersiz rol tanımları ve geçici bir makinede saklanan kimlik bilgileri neden olmaktadır.

Z.2- Kullanıcı Yapılandırma Zafiyetleri: Bu tehditlerin ana sebepleri arasında, müşterilerin kullanıcı yapılandırma sürecini kontrol edememesi ve buna bağlı olarak; müşteri kimlik bilgilerinin kayıt sırasında doğrulanmaması, bu bilgilerin çakışmaya ve tekrarlanmaya açık şekilde oluşturulması, kimlik verilerinin çoklu ve senkronlaştırılmamış kopyalarının tutulması ve bulut sistem bileşenleri arasındaki senkronizasyonda gecikmeler yaşanması örnek olarak gösterilebilir.

Z.3- Yeniden Yapılandırma Zafiyetleri: Tanımlanmış kimlik verilerini yürürlükten kaldırma hususunda meydana gelen gecikmeler nedeniyle, kaldırılmış kimlik bilgilerinin hala geçerli olması durumunda ortaya çıkarlar.

Z.4- Yönetim Arayüzüne Uzaktan Erişim: Tekil kullanıcı veya sağlayıcı tarafındaki istemler ve tepkilerle ilgili zayıf kimlik tanımlama nedeniyle, bulut altyapısının zayıflaması, son kullanıcı makinelerinde tehditlere yol açmaktadır. Yönetim

arayüzlerindeki zafiyetler, müşteri bilgilerine yetkisiz erişime sebep olabilir. Aynı zamanda bu düzeyde bir zafiyet, bir saldırganın bulut yapısı içindeki varlıklarda değişiklik yapmasına, hizmeti engellemesine, veri sızdırmasına veya sanal makinelerin birçok kopyasını çoğaltılıp piyasaya sürmesine neden olabilir.

Z.5- İtibar Ayrımı Eksikliği: Bu tehdit bir müşterinin faaliyetleri dolayısıyla, başka bir müşterinin kişisel veya kurumsal itibarının etkilenmesi yoluyla ortaya çıkar. Örneğin bir bulut sağlayıcısının hizmet platformu üzerinden kötü amaçlı aktiviteler gerçekleştiren müşterilerin varlığı, o platform üzerinden hizmet sunan diğer müşterilerin saygınlığını ve güvenilirliğini ister istemez etkileyecektir.

Z.6- Aktarılan Veri veya Arşivde Şifreleme Eksikliği veya Zayıflığı: Aktarılan verileri, arşiv ve veri tabanlarında tutulan verileri, çerçevelenmemiş sanal makine görüntülerini, adli görüntü ve verileri, hassas log kayıtlarını ve diğer verileri şifrelemede başarısızlık, bu verileri risk altına sokar. Bu sebeple şifre yönetimi uygulanmasının maliyeti ile işlem maliyetleri dikkate alınarak, bu riski önlemeye yönelik gerekli kontroller sağlanmalıdır.

Z.7- Veriyi Şifrelenmiş Biçimde İşlemenin Olanaksızlığı: Veri tabanlarındaki durağan veriyi şifrelemek kolaydır fakat şifrelemedeki son gelişmelere rağmen, işlem sırasında herhangi bir sisteme ait verilerin şifrelenmesi kullanılabilir değildir. Uzmanlar şifreli anahtar kelime ile internette arama yapmanın, aynı algoritmayla yapılan şifresiz bir uygulamanın işlem süresini yaklaşık bir trilyon kat artıracağını tahmin etmektedirler. Bu süre, işlemin efektif bir biçimde gerçekleştirilmesi için çok uzun olduğundan, bulutta veri depolayan bulut müşterilerinin sağlayıcının şifreleme prosedürüne bağlı kalması kaçınılmazdır.

Z.8- Zayıf Anahtar Yönetimi: Bulut bilişim altyapıları birçok farklı türde anahtarın yönetim ve depolanmasını gerektirir. Örnek olarak, aktarılan verileri korumak için oturum anahtarları, dosya şifreleme anahtarları, bulut sağlayıcıları belirleyen anahtar çiftleri, müşterileri belirleyen anahtar çiftleri verilebilir. Sanal makineler sabit donanım altyapısında olmadığından ve bulut tabanlı içerik coğrafi olarak dağıtılmış

olabileceğinden, bulut altyapılarının anahtarlarına, donanım güvenlik modülü (HSM) depolama gibi standart kontroller uygulamak zor olacaktır. Bunun sebepleri olarak, donanım güvenlik modüllerinin güçlü fiziksel korumalı olma zorunluluğu, karşılıklı hassas uzaktan kimlik doğrulama mekanizmalarının gerekliliği, dağıtılmış mimari içinde anahtarların iptalinin de pahalı olması ve yeni yetkililer oluşturmadaki kaynak yükü nedeniyle ortaya çıkabilecek ölçeklenebilirlik sorunları sıralanabilir.

Z.9- Standart Teknoloji ve Çözümlerin Eksikliği: Standartların eksikliği, verilerin bulut sağlayıcısına bağımlı olabileceği anlamına gelir. Bu durum, sağlayıcı bulut hizmetini sonlandırabileceğinden büyük bir risk olup; yönetilen mevcut güvenlik hizmetlerinin ve dış güvenlik teknolojilerinin kullanımını engellenebilir.

Z.10- Kaynak Emanet Anlaşması Eksikliği: Bu tehdit, Servis olarak Platform (PaaS) veya Servis olarak Yazılım (SaaS) sağlayıcısı iflas ederse veya hizmetlerini sonlandırırsa, bilişim kaynaklarında bulunan müşteri verilerinin korunmasına yönelik anlaşma bulunmaması durumunda ortaya çıkar.

Z.11- Kaynak Kullanımının Yanlış Modellenmesi: Bulut hizmetleri talebe bağlı olup, belli bir taahhüde bağlı olarak sağlanmadıklarından, kaynak tükenme risklerine karşı savunmasızdırlar. Kaynak tahsis algoritmalarındaki başarısızlık; kaynak kullanımının yanlış modellenmesi, olağanüstü olaylar, geçici aşırı yüklenmeler, kaynakların kötü sınıflandırılması sebeplerine bağlı olarak ilgili zayıflık ortaya çıkabilir.

Z.12- Güvenlik Açığı Değerlendirme Sürecinin Bulunmaması: Güvenlik açığı değerlendirmesi, bir sistemin açıklarının tanımlaması, ölçülmesi ve önceliklerine göre sıralanması işlemidir. Port tarama ise, bir sunucu veya ana bilgisayar üzerindeki açık portları tespit için tasarlanmış bir işlemdir. Bu işlem genellikle ağ yöneticileri tarafından, ağlarının güvenlik politikalarını doğrulamak için ve saldırganlar tarafından ana bilgisayarda çalışan servisleri tespit ve bunların zayıflıklarından istifade için kullanılır. Sağlayıcı tarafından port tarama ve güvenlik açığı testlerine ilişkin kısıtlamalar önemli bir zafiyet yaratırlar. Ancak, altyapı bileşenlerinin koruma sorumluluğunun müşteriye aktarılması da ciddi güvenlik sorunu yaratabilecektir.

Z.13- Adli Mevzuat Eksikliği: Bulut teknolojisi adli hazırlık geliştirme potansiyeline sahipken, birçok sağlayıcı adli mevzuata uygun hizmet veya bunu etkinleştirmek için kullanım şartları sunmaz. Örneğin, Servis olarak Yazılım (SaaS) sağlayıcıları genellikle, içeriği kullanan istemcilerin IP log kayıtlarına erişim izni vermeyecektir. Servis olarak Altyapı (IaaS) sağlayıcıları da sanal makine ve disk görüntülerine erişim gibi adli hizmetler vermeyebilir. Bu durum özellikle kurumsal müşterilerin adli işlemleri için bir tehdit oluşturmaktadır.

Z.14- Veri Silme ve Ortam Temizlemesi: Kişisel veya kurumsal olarak hassas (kişiye, hizmete özel) verilerin belli bir yaşam döngüsü sonunda imha edilmesi ile ilgili politikaların, fiziksel depolama kaynaklarının paylaşıldığı kiracılık sistemi nedeniyle uygulanması kolay değildir. Örneğin, disk yine başka bir kiracı tarafından kullanılıyorsa veya disk silme veya temizleme işlemi ile ilgili tanımlı bir prosedür bulunmuyorsa; bu ortamdaki verilerin sonradan hiçbir yöntemle erişilemeyecek şekilde yok edilmesi işlemi uygulanamayabilir.

Z.15- Gizli Bağımlılık Yaratan Alt Yükleniciler: Birçok bulut sağlayıcısı, farklı lokasyonlardaki belli başlı hizmetlerini alt yüklenicileri aracılığıyla sunmaktadırlar. Üçüncü şahısların dâhil olduğu bu hizmet tedarik zincirinde, müşteriler bu alt yüklenicilerden habersiz olsalar dahi, gizli bağımlılıklar ortaya çıkmaktadır. Bazı durumlarda alt yükleniciler servis sağlayıcıdan ayrıldığında, bulut sağlayıcı mimarisi ilgili işlemin sürekliliğini destekleyememektedir.

Z.16- Farklı Paydaşlara Verilen Sözlerle Çelişen Hizmet Seviye Anlaşması Hükümleri: Hizmet seviye anlaşması (SLA) hükümleri zaman zaman diğer hükümlerle veya diğer sağlayıcılardan alınan hizmet şartlarıyla çelişebilir. Bu sebeple hizmet seviye anlaşması imzalanmadan önce, bir diğer hükmü geçersiz kılan anlaşma maddeleri ve hizmetin taşere edilebileceği alt yüklenici ile sağlayıcı tarafından imzalanan anlaşma hükümleri dikkatle gözden geçirilmelidir.

Z.17- Aşırı İş Riski İçeren Hizmet Seviye Anlaşması Hükümleri: Hizmet seviye anlaşmaları hem sağlayıcı ve hem de müşteri tarafında önemli derecede iş riski

yaratabilecek hükümler içerebilir. Örneğin teknik arızaların yarattığı gerçek risk düşünüldüğünde, müşterinin kayıplarının tazmini ile ilgili hükümler bir sağlayıcı için çok fazla iş riski taşıyabilir. Aynı şekilde müşteri açısından bakıldığında, örneğin, hizmet seviye anlaşmasında fikri mülkiyet ile ilgili bir maddede, bulut sağlayıcının altyapısı üzerinde saklanan herhangi bir içeriğin telif hakkına sahip olduğuna dair bir hüküm, müşteri açısından ciddi zararlar ortaya çıkarabilir.

Z.18- Müşterilere Denetim ve Belgelendirme Yetkisi Verilmemesi: Birçok durumda sağlayıcı müşterilerine hizmetleri ile ilgili denetim ve belgelendirme hakkında herhangi bir güvence sağlamaz. İlgili sağlayıcının faaliyetlerinin müşteri veya müşterinin güvenebileceği bağımsız dış denetçiler tarafından denetlenmemesi, sağlayıcıyı büyük ölçüde kendi tanımladığı kontrol ve denetimlere yönelteceğinden, müşterilerin veri ve uygulamaları ile ilgili zafiyet oluşturmaktadır.

Z.19- Yetersiz Kaynak Sağlama ve Altyapı Yatırımları: Altyapı yatırımları bir sürece bağlı olarak ihtiyaçlar dâhilinde yapılmalıdır. Ancak bulut sağlayıcılar, müşterilerinin kaynak ihtiyaçlarını kesin bir şekilde hesaplayamadıklarından, zaman zaman özellikle de müşteri ihtiyaçları toplamının tepe değerlere ulaştığı zamanlarda; kaynak tedariği ve bunun sağlanması için de altyapı yatırımları hususunda yetersiz kalabilirler. Sağlayıcıların altyapı tedariği ile ilgili kullandıkları tahmini modeller başarısız olursa, bulut sağlayıcı hizmeti uzun süre aksayabilir.

Z.20- Kaynak Üst Limitleri ile İlgili Politika Belirlenmemesi: Müşterilerin kullandığı ve bulut sağlayıcıların sunduğu kaynaklar için, sınırlamalar koyabilmeye ve kaynak tedariğini bu sınırlar içinde esnek biçimde yapılandırabilmeye ilişkin bir karar alınmamışsa, kaynak kullanımı her iki taraf için öngörülemeyen boyutlara ulaşıp sorun yaratabilir. Müşteri maliyet açısından, sağlayıcı ise kaynak tedariği açısından zor durumda kalabilir.

Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği: Müşteriye sunulan gerçek zamanlı bilgi olmadan, verilerinin başka yargı mevzuatlarına tabi bölge veya ülkelerde bulunan veri merkezlerinde depolanması veya

yedeklenmesi durumlarında, verilerin depolandığı yere göre güvenlik açıkları oluşabilir. Verilerin depolandığı bölgelerin yargı mevzuatı hakkında sağlayıcı şirketlere net bilgi sağlanmamışsa, şirketler bilmeden bu mevzuat hükümlerini ihlal edebilirler.

Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği: Bazı ülke veya bölgelerde veriye zorla erişilmesine veya el koyulması imkân tanıyan, yüksek riskli yargı mevzuatları geçerlidir. Verilerin sağlayıcı tarafından bu tip riskler bulunan bölgelerde depolanması veya işlenmesi nedeniyle, verilerin gizliliği ve güvenliği tehlikeye girebilir. Eğer müşterinin verilerinin bu tip bölgelerde depolandığına dair bilgisi yoksa ilgili yasal girişimleri önlemek için adımlar atamayacaktır.

Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği: Bulut bilişim hizmetlerinin kullanımı ile ilgili talep ve taahhütleri kayıt altına alan hizmet seviye anlaşmaları, sağlayıcı tarafından genellikle kendisini korumaya yönelik ve tek taraflı olarak hazırlanmıştır. Bu anlaşmalarda, sağlanan bulut hizmeti ile ilgili karşılaşılabilecek bir takım sorunlara ilişkin gerekli hükümler, sağlayıcıya ek bir maliyet yaratmama adına eklenmemekte ve bu durum müşteriler için önemli bir tehdit unsuru ortaya çıkarmaktadır.

3.3.2. Bulut Bilişime Özel Olmayan Tehdit ve Zafiyetler

Aşağıdaki tehditler bulut bilişime özgü olmasa da, bulut bilişim hizmetlerini doğrudan etkileme potansiyeli taşımaları nedeniyle ele alınacaktır.

T.9- Kaynak Tüketim Tehditleri: Bulut bilişim kaynak kullanımında talebe göre self servis politikası uygulayan bir hizmet modelidir. Bu durum, sağlayıcılar açısından müşterilerinin kullanacağı kaynak miktarını hesaplamayı zorlaştırmaktadır. Müşteriler ise genelde bulut üzerinden sundukları hizmetlerinin yaratacağı işlem yükünü ve veri trafiğini öngörebilecek nitelikte değildir. Bu sebeple sağlayıcı, eğer kullanım başına ücret ödeyecek olan müşterilerinin kullanacağı olası toplam kaynak miktarını yanlış öngörür veya hesaplarsa, ya çok fazla altyapı ayıracağı için kaynakları atıl kalacak veya gereğinden az öngörmesi durumunda altyapı kaynağı yetersiz kalacaktır. Aynı şekilde, bulut sağlayıcısı ile kullanacağı kaynak miktarı ile ilgili alt ve üst limitlere dair bir

anlaşmaya varan bir müşteri de, ihtiyacı olan kaynak miktarını yanlış öngörmesi durumunda benzer tehditlerle karşılaşacaktır.

T.10- Sağlayıcının Gizlilik Sözleşmesi İhlali: Tanım olarak Gizlilik Sözleşmesi, taraflar arasında yürütülen proje ya da paylaşılan iş konusu ile ilgili olarak, gizlilik içerdiği açıkça belirtilen bilgi ve belgenin, ilgili kişinin onayı alınmadıkça herhangi bir üçüncü gerçek ve/veya tüzel kişiye açıklanmamasını temin edecek olan gizliliğin sınırlarının ve koşullarının belirlenmesidir. Bulut bilişimde bu sözleşme, müşteriye sağlayıcıyla paylaştığı veri ve uygulamaları ile ilgili kontrol hakkı sağlar. Sağlayıcının bu sözleşmeyi ihlal etmesi veya gizliliğe esas veri ve teknik bilgilerin korunması yönünde çaba göstermemesi durumunda, tazminat ile cezalandırılması gerekecektir. Ancak çeşitli ülkelerdeki yasal uyumsuzluklar veya sağlayıcının iflası, şirketinin el değiştirmesi gibi çeşitli durumlar, ilgili Gizlilik Sözleşmesi'nin ihlal edilmesine ortam hazırlayabilecek olup; bu durum müşteri verilerinin ifşasına yol açabileceğinden ciddi bir tehdittir.

T.11- Kötü Sağlayıcı Seçimi: Bulut bilişim hizmet seçiminde (özellikle de SaaS) önemli tehditlerden bir tanesi, çok farklı sektörler ve disiplinler için hizmet geliştiren bulut bilişim sağlayıcılarını karşılaştırmanın zor bir süreç olmasıdır. Sağlayıcı seçiminde teklif edilen fiyat ve kaynakların performanslarına ek olarak; hizmetin kullanılabilirliği, güvenliği, müşteriler ile sağlayıcı arasındaki iletişim hatlarının kalitesi, sağlayıcının piyasa itibarı, yasal ve kurumsal faktörler gibi birçok faktör dikkate alınmalıdır. Ayrıca sağlayıcının mevcut müşterilerinin güveni, sağlayıcı seçiminde önemli bir faktördür. Yine sağlayıcıları seçerken piyasa deneyimi, teknik uzmanlık, kredi imkânları ve şirket istikrarı gibi konulara da dikkat edilmelidir. Aksi takdirde, müşteri kurum veya kuruluşun sunacağı hizmete uygun olmayan veya yukarıda belirtilen kriterler ile ilgili gereksinimleri karşılamayacak olan bir sağlayıcının seçimi; sunulan hizmetin erişilebilirliği, kullanılabilirliği, idamesi ve güvenliği gibi birçok konuda tehditler ortaya çıkarabilecektir.

T.12- Yanlış Yapılandırma: Bu tip tehditler temel ve ileri seviye güvenlik tedbirlerinin yetersiz seviyede uygulanması, insan hatası ve veri merkezi yöneticilerinin yeterli seviyede eğitim almamış olması sebebiyle ortaya çıkabilmektedir.

T.13- Sistem veya İşletim Sistemi Tehditleri: Bu tip tehditler bulut yönetim, izleme, kontrol, güvenlik yazılımlarındaki açıklar ve yanlış yapılandırma kusurları sebebiyle ve ayrıca kullanılan işletim sisteminin bulut altyapısının sistem veya güvenlik gereksinimlerini karşılayamadığı durumlarda ortaya çıkan tehditlerdir.

T.14- Güvenilmeyen Yazılım: Bu tehdit sağlayıcı tarafında gerekli güvenlik prosedürlerini sağlamayan hipervizör, işletim sistemi, uygulama, izleme, kontrol ve güvenlik yazılımları sebebiyle ortaya çıkmaktadır.

Z.24- Güvenlik Gereksinimleri Farkındalık Eksikliği: Bazı bulut müşterileri, bulutun içine veri ve uygulamalarını aktardıklarında; kontrol kaybı, sağlayıcı bağımlılığı, tükenmiş sağlayıcı kaynakları vb. buluta özgü tehditler sebebiyle karşıya kalabilecekleri risklerin farkında değildir. Müşterinin bu farkındalık eksikliği, bu riskleri azaltmak için alınması gereken eylemlerin farkında olmayan bulut sağlayıcısını da etkileyebilir.

Z.25- Güvenlik Araştırması Süreçlerinin Eksikliği: Bulut sağlayıcılarının personeli içinde, mimarinin büyük ölçeği sebebiyle çok yüksek ayrıcalığa sahip roller olabileceğinden, bu tür rollere sahip personelin güvenlik araştırması risk profili olmaması veya yetersiz olması önemli bir zafiyettir. Kötü niyetli ve yüksek ayrıcalıklı sağlayıcı personelinin, çok sayıda müşterinin önemli miktarda veri ve uygulamasına zarar verebileceği ve veri gizliliği gerektiren bilgileri ifşa edebileceği düşünüldüğünde; bu kişilerin işe alım sırasında çok miktarda güvenlik soruşturmasına tabi tutulması gerektiği açıkça ortaya çıkacaktır.

Z.26- Belirsiz Görev ve Sorumluluklar: Bu zafiyetler, bulut sağlayıcı kuruluşta rollerin ve sorumlulukların yetersiz atanması sonucu ortaya çıkmaktadır. Yetki ve sorumlulukların pozisyona göre atanmaması, yüksek ayrıcalıklı kullanıcılara ait giriş

şifrelerinin yetki tanımı bulunmayan personelce de kullanılması önemli zafiyetlere sebebiyet vermektedir.

Z.27- Zayıf Rol Tanımı Uygulamaları: Bulut sağlayıcı içinde rollerin atanmasında meydana gelen başarısızlık, aşırı ayrıcalıklı roller tanımlanmasına yol açabilir ve bu durum çok büyük sistemlerin savunmasız kalmasına neden olabilir. Örneğin, bulut mimarisindeki tüm veri ve uygulamalara erişim ayrıcalığı tek bir kişiye verilmemelidir.

Z.28- Gereksiz Yetkiler Verilmesi: Bu tehdit hem müşteri ve hem de sağlayıcı personeli için, gerekenden fazla ayrıcalıkta ve sayıda kişiye tanınan ayrıcalıklı roller ve sorumluluklar ile ortaya çıkmaktadır. Her iki tarafta da gereksiz yere verilere erişim yetkisi verilmemeli, roller birbirinden ayrılmalı ve mümkün olduğunca az personele atanmalıdır. Aksi takdirde her yeni ayrıcalıklı personel ek risk oluşturmaktadır.

Z.29- Yetersiz Fiziksel Güvenlik Prosedürleri: Müşterilerin verilerinin barındırıldığı veri merkezlerinin fiziksel güvenliği önemli bir tehdit unsurudur. Bu duruma yönelik tehditler, akıllı kart veya biyometrik kimlik doğrulaması ile veri merkezine giriş çıkışların kontrolünün sağlanmaması ve tesis dışından dinlenebilecek kritik cihazlar için elektromanyetik koruma tedbirlerinin alınmaması gibi güvenlik tedbirlerine bağlı olarak ortaya çıkarlar.

Z.30- Yetersiz İş Sürekliliği ve Felaket Kurtarma Planı veya Eksikliği: Bulut bilişimde felaket kurtarma, bir güvenlik önlemi olarak, bir bulut bilişim ortamındaki elektronik kayıtların kopyalarının depolanmasını ve muhafazasını içeren bir yedekleme ve geri yükleme stratejisidir. Bu stratejinin hedefi, insan eliyle veya doğal bir afet durumunda kaybedilen verileri kurtarmak veya yük devretmeyi uygulamak için kuruluşa bir çözüm sağlamaktır. Bulut bilişimde iş sürekliliği planlaması ise, potansiyel tehditlerle başa çıkmak için önleme ve kurtarma sistemleri oluşturma sürecidir.

Bulut tabanlı bir felaket kurtarma ve iş sürekliliği çözümü, kesinti ve veri kaybı ile ilgili düşük toleransa sahip işler için son derece önem taşır. Günümüzde birçok KOBİ de dâhil olmak üzere büyük işletmeler; işlem odaklı, veri yoğun ve zamana

duyarlı işlemler yürütmektedirler. Birçok işletme ve örneğin hastaneler gibi kritik servis sağlayıcıların servisleri hiç zaman çökmemeli ve iki ya da üç dakikadan daha uzun veri kaybına uğramamalıdır. Bu sebeple bulut mimarileri gibi birçok farklı sektörün aynı altyapı üzerinden hizmet verebileceği sistemlerin çökmesi veya veri kaybına uğraması, çok sayıda müşteri ve bu müşterilerin hizmet sunduğu kullanıcıları etkileyebileceğinden; yeterli iş sürekliliği ve felaket kurtarma planı bulunmaması önemli bir tehdit unsurudur.

Z.31- Eksik veya Hatalı Varlık Envanteri: Bir kuruluşta varlıkların belirlenmesi ve varlıklara değer atanması, risk analizi süreci için temel bir adımdır. Varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. Organizasyon içinde bir "varlık yönetim kılavuzu" veya "varlık envanteri yönetim kılavuzu" hazırlanmasında fayda vardır. Bu kılavuzda özellikle envantere yeni bir varlığın eklenmesi, envanterden varlık çıkarılması ve envanter sorumlusu net olarak belirtilmelidir. Bilgi güvenliği açısından bir donanımın bütünlüğünden söz etmek çok zordur. Bu sebeple asıl korunması ve yönetilmesi gereken bilgi veya süreçleri değerlendirmek, ardından bu bilgi ve süreçleri sağlayan veya barındıran donanım ve yazılımı güvenlik açısından incelemek ve sınıflandırmak daha kolay olacaktır. Diğer varlıklar düşünüldüğünde (yazılım, donanım, fiziksel varlıklar ve insan), bilgi ve süreçler en soyut kavramlardır ve güvenliğin üç temel öğesi (gizlik, bütünlük, erişilebilirlik) için derecelendirmenin kolaylıkla yapılabileceği varlık gruplarıdır (Koç, 2008). Bu sebeplerle bulut bilişim mimarilerinde varlık envanteri eksikliği; risk analizini, risk yönetimini ve dolayısıyla risk yönetimini temel alan Bilgi Güvenliği Yönetim Sistemi'nin uygulanmasını imkânsız hale getirecektir. BGYS'nin bilişim mimarilerilerinde uygulanmaması tüm yazılım, donanım ve diğer fiziksel varlıklar için risk olasılıklarını artırır.

Z.32- Eksik veya Hatalı Varlık Sınıflandırması: Bir kuruluşta varlık envanteri belirlendikten sonra, ilgili envanterde bulunan varlıkların sınıflandırılması ve varlık sınıflarına göre yönetilmesi önem arz etmektedir. Böylece her varlık sınıfının gereksinimlerine göre bir yönetim stratejisi belirlenecek ve ilgili varlıkları tehdit edecek riskler ilgili sınıfa göre değerlendirilecektir.

Z.33- Varlık Mülkiyeti Belirsizliği: Varlık mülkiyeti tanımlama, ilgili varlığı etkileyen bütün işlemler hakkında o varlıktan sorumlu yönetici veya danışmanın bilgilendirilmesini sağlar. Bu sayede varlığın örneğin geçici veya sürekli olarak hizmet dışı bırakılması durumunda, varlık sahibi rol tabanlı onay sürecindeki pozisyonuna göre bu işlemi yürütür veya bu konuda bilgilendirilir. Örneğin bir sunucu varlığı üzerinde üç adet uygulamanın çalıştığını ve her bir uygulama için bir operatör bulunduğunu düşünecek olursak, ilgili uygulamalarda sunucu kaynaklı bir sorun olması durumunda, uygulama operatörlerinin başvurması gereken kişi o sunucudan sorumlu personel olan varlık sahibi olacaktır. Ancak varlık mülkiyetinin belirsiz olduğu durumlarda, o varlıkta meydana gelen sorunlar nedeniyle etkilenen müşteriler veya iç kullanıcılar muhattap bulmakta zorlanırlar ve bu da ciddi hizmet kesintisi tehditlerini beraberinde getirir.

Z.34- Proje Gereksinimlerinin Eksik Belirlenmesi: Bu tehdit bulut müşterilerinin hizmet ve uygulamalarını buluta aktarmadan önce, öncelik ve gereksinimlerini eksik veya hatalı belirlemeleri sonucu ortaya çıkar. Örneğin yasal olarak veri gizliliği gerektiren kişisel kimlik bilgilerinin veya banka hesap numaralarının tutulduğu uygulamalar için, güvenlik ve yasal uyumluluk gereksinimleri değerlendirilmeden bu uygulamaların bulut mimarisine aktarılması; bu uygulamaların yasal şartları taşımadıkları için kullanılamaması sonucunu doğurabilir. Aynı şekilde hedef kitlesi, işlem yükü ve iş gereksinimleri doğru belirlenmeden buluta aktarılan uygulamaların kullanılabilirliği ile ilgili ciddi tehditler ortaya çıkabilir.

Z.35- Sağlayıcı Yedeklilik Eksikliği: Sağlayıcı yedekliliği, müşteri tarafından alınan hizmetin devamlılığı açısından çok önemlidir. Tek bir sağlayıcıya bağımlı kalmak, istendiği takdirde hizmet seviye anlaşmasını fesh edip uygulama ve verilerini bir başka sağlayıcının alt yapısına aktaramamak, müşteriler için ciddi bir sorundur. Örneğin sağlayıcının iflası veya hizmet şeklini değiştirmesi durumunda, müşteri uygulamaları bir anda kullanılamaz hale gelebilir. Aynı şekilde sağlayıcı, kendine bağımlı hale gelen müşteriye uyguladığı fiyatlandırma politkasında zaman içinde müşteri aleyhine değişikliğe gidebilir. Bu ve bunun gibi durumlar sağlayıcı yedekilik eksikliğini müşteri açısından ciddi bir tehdit haline getirmektedir.

Z.36- Kötü Yama Yönetimi ve Uygulama Açıkları: Yama yönetimi, ağ güvenliğini korumak için bir kurumun BT altyapısındaki açıkları tamir sürecidir. Ayrıca altyapı açıklarının yanısıra uygulamalara ilişkin açıklar da uygun yamalar kullanılarak düzeltilebilir. Bu yazılım veya yamalar, stratejik olarak uygulamalara, eklentilere, yazılımlara, sunuculara ve BT altyapısının diğer bileşenlerine yüklenirler. Ancak yama yönetimi zaman, personel ve kaynak gerektirdiğinden, küçük ve orta ölçekli işletmeler, (KOBİ'ler) altyapı ve uygulamalarının güvenlik açıklarının düzeltilmesinde çoğu zaman etkisiz kalmaktadırlar.

Yama yükleme politikaları yapılandırıldıktan ve yazılımın envanteri çıkarıldıktan sonra, yama yönetimi için oluşturulan araçlar işlemi otomatikleştirmeyi sağlayabilecektir. Yamalara öncelik verilmesini, test edilmesini, planlanmasını ve güncel tutulmasını sağlamak kritik öneme sahiptir ve böylece kuruluş masraflı kesintilere ve veri kaybına neden olabilecek güncel tehditlere karşı korunmuş olacaktır (The SageNet Team, 2015).

Ancak uygulama kodu bugları, sağlayıcı ve müşteri arasındaki birbirine aykırı yama işlemleri, denenmemiş yamaların uygulanması, tarayıcılardaki güvenlik açıkları vb. sebepler yetersiz yama yönetimi tehdidini ortaya çıkarmaktadırlar.

Z.37- Sağlayıcının Veri Kaybına Karşı Sorumluluğu: Veri kaybının temel türleri arasında verinin imhası, bozulması ve yetkisiz veri erişimi bulunmaktadır. Bu kayıpların sebepleri arasında altyapı arızaları, yazılım hataları ve güvenlik ihlalleri yer almaktadır. Verileri korumak ve kaybını en aza indirmek amacıyla uygulanabilecek yöntemler arasında; disk düzeyinde veri koruma, yedekleme veya çoğaltılmış yedekleme, veri çoğaltma ve günlük veya kontrol noktası tabanlı çoğaltma yer almaktadır. Ancak sağlayıcı bu yöntemleri hiç veya yeterli düzeyde uygulamazsa, yaşanabilecek veri kayıpları müşteri açısından ciddi zafiyet oluşturabilir.

Z.38- Log Kayıtları ile İlgili Politika ve Prosedürlerin Eksikliği: Log kaydı; tüm işlem hareketlerinin birer birer kayıt altına alınmış olduğu dosyalardır. Örneğin bir web sunucusunun içerisinde yer alan log dosyaları incelenerek, ziyaretçilerin nereden geldiği

ve web sunucusuna hangi istekleri gönderdiği kolaylıkla anlaşılabilir. Log dosyaları iyi birer analiz aracı olabileceği gibi, sorun teşhisi konusunda da oldukça faydalı kayıtlardır. Örneğin bir bilgisayarın işletim sisteminin üretmiş olduğu log kayıtları incelenerek, sistemde meydana gelen sorunun neden kaynaklandığı öğrenilebilir ve buna göre çözümler üretilebilir. Ancak log kayıtlarının yetersiz tutulması veya tutulan kayıtların uygun şekilde saklanmaması, hem yapılan işlem geçmişinin kaybolmasına ve hem de sistemde meydana gelen sorunların kaynağına inilememesine yol açacaktır.

Z.39- Yetersiz Filtreleme Kaynakları: Bilişimde filtreleme, belirli kriterlere göre her giriş veya çıkış isteğini incelemek ve buna göre işlemek veya iletmek için tasarlanmış bir program veya kod bölümüdür. Çok fazla sayıda kullanıcının giriş çıkış yaptığı ve çok hızlı bir veri akışının bulunduğu bulut bilişimde; istenilmeyen veri, kod veya erişimlerin filtrelenmesi, veri güvenliği ve hizmetin sürdürülebilirliği açısından kritik öneme sahiptir. Url filtreleme, spam filtreleme, veri paketi filtreleme, IP filtreleme, port filtreleme, web filtreleme, içerik filtreleme gibi değişik veri filtreleme yöntemleri mevcuttur. Sağlayıcının filtreleme konusunda eksik veya ilgisiz kalması veri güvenliği ve gizliliği için ciddi tehditler oluşturabilir.

3.4. Bulut Bilişimde Riskler

Esnek yapısı, talebe bağlı olarak kolayca ölçeklenebilirliği, ilk kurulum ve işletme maliyetlerine katkıları vb. birçok özelliği göz önüne alındığında; günümüzde en uygun ve mantıklı bilgi teknolojisi çözümü olmasına rağmen, bulut teknolojileri bir takım riskleri de beraberinde getirmektedir. Bu risklerin çoğu, hâlihazırda kullanılan geleneksel sistemlerde de mevcuttur.

Farklı mimarilerde ve farklı servis modellerinde hizmet veren geniş bir portföye sahip bulut bilişimden, herhangi bir kamu kurum ve kuruluşunun nasıl en etkin bir biçimde faydalandırılabileceğine karar vermenin yolu; kurumun sunduğu hizmetlerin her bir mimari veya servis modeli üzerinde sunulmasının sağlayacağı faydalar ve kurum için yaratacağı risklerin birlikte değerlendirilerek, en kârlı ve optimal çözümün seçilmesidir. Örneğin gizlilik derecesi yüksek veya kişiye özel verilerin, veri ifşası riski göz önünde

bulundurularak özel bulut mimarilerinde barındırılması ve işlenmesi, kamuya açık veri ve uygulamaların açık bulutlarda sunulması, her iki hizmet türünde veri ve uygulamaları olan kuruluşların ise hibrit bulut modelini kullanarak, hem bulut bilişimin avantajlarından üst düzeyde yararlanıp hem de veri güvenliğini üst düzeyde tutabilmeleri, bulut mimarilerinin hizmet türüne göre mimari seçme esnekliğini yansıtmaktadır.

Bulut bilişimin büyük bir kaynak, veri ve uygulamalar kümesi olması sebebiyle; bu altyapılarının saldırıya maruz kalma ihtimali kurum içi geleneksel mimarilere göre daha yüksektir. Bu nedenle bulut mimarilerinde güvenlik gereksinimleri daha yüksektir. Bu sebeple herhangi bir saldırının sisteme zarar vermesini engellemek veya zararı minimize etmek için, bulut servis sağlayıcılarının önemli ölçüde güvenlik yatırımı yapması gerekmektedir. Yine bu mimarileri kullanan kamu kurum ve kuruluşlarının varsa hizmet sağlayıcılarıyla birlikte çeşitli alanlarda oluşabilecek riskleri önceden belirleyip, bu riskler karşısında alacakları aksiyonları ve iyileştirme çalışmalarını belirlemeleri, bu risklerin neden olabileceği zararları minimize edebilecektir.

Bulut bilişim dünyasında karşılaşılabilecek başlıca riskler; Kurumsal ve Stratejik Riskler, Teknik Riskler ve Güvenlik Riskleri, Hukuksal Riskler ve Buluta Özgü Olmayan Diğer Riskler olarak sınıflandırılmış olup, bu riskler aşağıda kısaca açıklanmıştır.

3.4.1. Kurumsal ve Stratejik Riskler

R.1- Yönetim ve Kontrol Kaybı: Bulut mimarilerinde müşteriler genellikle, veri ve uygulamalarının güvenliği, gizliliği ve kullanılabilirliği ile ilgili bir dizi konuda kontrolü sağlayıcıya devretmek zorunda kalabilirler. Veri, uygulamalar ve kaynaklar tamamen sağlayıcı tarafında yer alacağından (özellikle açık bulut mimarilerinde), kullanıcı erişim kontrolü kuralları, güvenlik politikaları ve bunlarla ilgili kısıtlamalar bulut sağlayıcı tarafından yönetilir. Ayrıca müşteriler veri güvenliği ve gizliliği, kaynak kullanılabilirliği, hizmetler ve kaynakların izlemesi ve onarımı gibi birçok konuda sağlayıcıya güvenmek zorunda kalabilirler (Turahi, 2013).

Bunun yanında hizmet seviye anlaşmaları (SLA); müşterilerin port taramaları, güvenlik açığı değerlendirmeleri ve penetrasyon testleri gibi veri güvenliği amaçlı faaliyetlerine engel teşkil edip; bu hizmetleri sağlamak için bir taahhüt sunmayarak bir güvenlik boşluğu yaratıyor olabilir. Ayrıca sağlayıcı, taahhüt ettiği ilgili hizmetleri kendisi tarafından garanti edilen hizmet şartlarını sunmayan bir dış sağlayıcı veya taşeron şeklindeki üçüncü kişiye yaptırıyor olabilir. Diğer bir seçenek olarak, bulut sağlayıcının kontrolünün değişmesi sebebiyle hizmet şartları da değişebilir.

Yönetim ve kontrol kaybı, kuruluşun müşterilerine veya vatandaşlara taahhüt ettiği hizmet kalitesi ve hedeflerine yönelik stratejisi ve dolayısıyla itibarı ve kapasitesi üzerinde olumsuz sonuçlar yaratabilir. Bu risk güvenlik gereksinimleri ile uyumsuzluğa, verinin gizlilik, bütünlük ve kullanılabilirliğinde eksikliğe, performans ve hizmet kalitesinde bozulmaya ve yasal uyum problemlerine neden olabilir.

R.2- Bulut Hizmeti Sonlandırması veya Arızası: Olumsuz piyasa koşulları, mali yetersizlikler, aşırı rekabet gibi hususlar nedeniyle, bulut sağlayıcıları hizmetlerini sonlandırabilir veya yeniden yapılandırabilirler. Eğer sözleşmelerde hizmetin süresi ile ilgili taahhütler verilmemiş ve cezai şartlar konulmamışsa, hizmet sonlandırma veya uzun süreli arıza durumları bulut müşterisi için; kendi hizmetlerinin sunum performansında ve kalitesinde kayıplara ve ayrıca bulut yatırımı için kullandığı ödeneğin kaybına yol açabilir.

Ayrıca yine sağlayıcı tarafından sunulan hizmetlerde meydana gelen problemler, bulut müşterisinin kendi müşterilerine karşı olan görevlerini ve yükümlülüklerini karşılamasını zora sokabilecektir. Müşteri kurum veya kuruluş, sağlayıcının ihmali dolayısıyla kendi müşterilerine karşı sözleşmeye dayalı sorumluluklara maruz kalabilir. Yine bulut sağlayıcısı kaynaklı hatalar sebebiyle müşteri, çalışanlarına karşı da haksız sorumluluklar yüklenebilir.

R.3- Servis Sağlayıcı Bağımlılığı: Her bulut bilişim servis sağlayıcısı, verileri kendine özgü formatlarda saklar ve kendine has kullanım biçimleri olan uygulama ve ara yüzlerle kullanıcılarına hizmet verir. Bu nedenle, belirli bir servis sağlayıcı üzerinde yer

alan veri ve uygulamalar başka bir servis sağlayıcıya taşınmak istendiğinde, uyum problemleri ile karşılaşılabilmektedir. Hizmet alınan servis sağlayıcıya bir anlamda bağımlılık söz konusudur. Bağımlılık riskini en aza indirmek için servis sağlayıcı tercihi doğru biçimde yapılmalı, verileri genel kabul gören standartlarda ya da en azından çözümlenebilir ve dönüştürülebilir standartlarda saklayan servis sağlayıcılar tercih edilmelidir.

Sağlayıcı bağımlılığı farklı bulut servis modellerinde farklı özellikler göstermektedir. Servis olarak Yazılım (SaaS) hizmetlerinde, müşteri verileri genellikle sağlayıcı tarafından tasarlanan özel bir veritabanı şemasında saklanır. Çoğu sağlayıcı, veri kayıtlarını okumak için ve dolayısıyla aktarmak için API çağrıları sunarlar. Ancak, eğer sağlayıcı hazır veri aktarım metodu sunmuyorsa, müşteri veri ve uygulamalarını başka bir sağlayıcıya aktarmak istediğinde; verilerini mevcut bulut içinden ayıklamak için bir program geliştirmesi ve başka bir sağlayıcıya aktarım için hazır dosya yazması gerekecektir. Yeni sağlayıcı normalde belli bir maliyetle bu çalışmaya yardımcı olabilir. Ancak, kurum içi verinin geri getirilmesi gerekiyorsa ve mevcut sağlayıcı böyle bir prosedür sunmuyorsa, müşterinin herhangi bir gerekli veri gönderimi için bilgi alım prosedürleri hazırlaması gerekir.

Uygulama bağımlılığı, bağımlılığın en belirgin şekli olup, SaaS sağlayıcıları genellikle hedef pazarın ihtiyaçlarına özel uygulamalar geliştirirler. Geniş bir kullanıcı tabanı ile SaaS müşterileri, başka SaaS sağlayıcıya geçiş yaparken son kullanıcıların farklı bir uygulamayı kullanmaları gerekeceğinden, çok yüksek eğitim giderleri ile yüzleşebilirler. Ayrıca müşteri, doğrudan sağlayıcının API'leri ile etkileşim sağlayacak programlar geliştirmişse, bütün bunların yeni sağlayıcının API'si dikkate alınarak yeniden yazılması gerekir.

Servis olarak Platform (PaaS) servislerinde bağımlılık hem API katmanı hem de bileşen düzeyinde meydana gelir. Örneğin, PaaS sağlayıcı yüksek verimli bir arka plan veri deposu sunabilir. Burada, müşterilerin sağlayıcı tarafından sunulan özel API'leri kullanarak kod geliştirmek zorunda olmaları yanında, bu arka plan veri deposu ile

uyumlu veri erişim prosedürleri kodlamaları gerekir. Veri erişim modeli farklı olacağından, görünüşte uyumlu bir API teklifinde bile, bu kodun mutlaka PaaS sağlayıcıları arasında taşınabilir olduğu garanti edilemez (Catteddu, 2009).

Servis olarak Altyapı (IaaS) bağımlılığı, tüketilen altyapı hizmetlerine bağlı olarak değişir. IaaS bilişim sağlayıcıları genellikle hipervizör tabanlı sanal makineler sunar. Sağlayıcılar arasında aktarılan ve taşınabilirlik için birlikte paketlenmiş olan yazılım ve metaveri; açık standartlar (örneğin OVF (11)) sağlanıncaya kadar tipik olarak sadece mevcut IaaS sağlayıcının bulutu içinde anlamlıdır.

IaaS sağlayıcıların sundukları depolama hizmetleri, basit anahtar ve değer temelli veri depolarından; belli bir politikaya göre geliştirilmiş dosya tabanlı depolara kadar değişir. Özellik setleri ve dolayısıyla depolama semantiği önemli ölçüde değişebilir. Ancak, uygulama seviyesinin belirli politikalara bağımlılığı, müşterinin sağlayıcı seçimini sınırlayabilir. Veri bağımlılığı, IaaS depolama hizmetlerinde belirgin bir husustur. Bulut müşterileri bulut depolama içine daha fazla veri yükledikçe, eğer sağlayıcı veri taşınabilirliği sağlamıyorsa veri bağımlılığı artar (Catteddu, 2009).

R.4- Üçüncü Parti Tedarikçi Hatası: Sağlayıcılar müşterilerine sundukları hizmetlerin bazılarını, üçüncü parti firmalara taşere edebilmektedirler. Özellikle dünyanın farklı lokasyonlarında hizmet sunan küresel ölçekli sağlayıcılar, bazı ülkelerde, o ülkenin yerel hizmet sağlayıcılarının altyapılarından faydalanabilmektedir. Böyle bir durumda bulut sağlayıcısının güvenlik seviyesi, kullandığı taşeron firmaların her birinin güvenlik düzeyine ve bulut sağlayıcısının bu firmalara bağımlılık düzeyine bağlıdır. Hizmet tedarik zincirinde yaşanabilecek herhangi bir kesinti veya arıza; tüm tarafların kendi müşteri veya kullanıcılarına karşı olan sorumluluklarını yerine getirememesi sonucunu doğurur. Bu durumda son kullanıcıların; hizmetlere erişememesi, verilerinde gizlilik, bütünlük ve kullanılabilirliğin kaybı, taleplerinin karşılanamaması gibi nedenlerle; kuruluşların maliyet ve itibar kayıpları ve hizmet seviye anlaşmalarının ihlali gibi olumsuz sonuçlar ortaya çıkabilir.

Bulut sağlayıcılar kâr amaçlı kuruluşlar olduklarından ve hizmetleri taşere edecekleri alt yüklenici kuruluşlar fiyat rekabeti dolayısıyla sürekli değişebileceğinden; genel olarak sözleşmelerde BT hizmetinin hangi alt yükleniciden sağlandığını beyan ve taahhüt etmek istemezler. Ancak bu durumda müşteri kuruluş, veri ve uygulamalarının kimin tarafından barındırıldığını veya işletildiğini bilemeyeceğinden, karşı karşıya kalabileceği riski değerlendiremeyecektir.

R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması: Bulut sağlayıcı kuruluşun başka bir firmaya satılması, müşteri ve sağlayıcı arasındaki bağlayıcılığı olmayan sözleşme dışı veya sözlü anlaşmaların geçerliliğini tehlikeye sokabilecektir. Bu nedenle örneğin yazılım arayüzleri, güvenlik yatırımları veya sözleşme dışı güvenlik kontrolleri gibi konularda meydana gelebilecek değişiklikler; müşteri kuruluşun hizmetlerinin kullanılabilirliği, güvenilirliği ve dolayısıyla keni müşterilerine karşı itibarı açısından olumsuz sonuçlar doğurabilecektir.

R.6- Uyum Sorunları: Buluta geçiş yapan bazı kuruluşlar, rekabet avantajı sağlamak veya endüstriyel standartları ve düzenleyici gereksinimleri karşılamak için, belgelendirmeye önemli yatırımlar yaparlar. Ancak burada sağlayıcının, ilgili belgelendirme için sahip olması gereken kurallara uygun şekilde hizmet verdiğini kanıtlayamama veya bu kurallara ilişkin müşterinin denetimine izin vermeme durumları ciddi bir risk oluşturur. Bu durum kurum veya kuruluşun ilgili standartlara uyum sağlanamaması sebebiyle, sunduğu hizmetleri veya bu hizmetlerin belli kısımlarını kullananaması sonucunu doğurabilir. Örneğin, hesap verisi korumaya ilişkin güvenlik standartları olan *PCI standartlarına uymayan hizmetlerin, kredi kartı işlemlerinde kullanılamaması dolayısıyla; kurum ve kuruluşların ilgili hizmetlerine yönelik ödeme işlemlerinin kredi kartıyla gerçekleştirilememesi gibi durumlar oluşabilir.

Bulut sağlayıcıların, müşterilerine barındırdıkları veri ve uygulamalar için bilgi güvenliği ile ilgili kontrollerinin varlığını kanıtlamaları gerekir. Aynı durum kendi bulutlarını oluşturan ve kendi denetimlerini kendileri yapan kuruluşlar için de geçerlidir.

*PCI Security Standards Council: Hesap verisi korumaya ilişkin güvenlik standartlarının sürekli gelişimi, geliştirilmesi, depolanması, yayılması ve uygulanmasına yönelik açık bir küresel forumdur.

Zira çoğu denetçiler, sanallaştırma veya bulut bilişim teknolojilerine hâkim olmadıklarından, veri güvenliği ve gizliliği ile ilgili denetimlerde yetersiz kalmaktadırlar. Bulut sağlayıcıları, bulut ortamlarında kontrol etkinliği için **SAS 70 tip II denetim raporları oluşturmaktadırlar fakat çoğu güvenlik ve uyum uzmanları bu raporları yetersiz bulmaktadır. Bunun başlıca sebebi, bu denetimlerin büyük ölçüde kendinden tanımlı ve aynı zamanda kontrollerin denetimlerinin nasıl yapıldığına ilişkin belirsizlikler içermeleridir. Birçok alanda en iyi denetim uygulamaları için yapılandırılmış bir çerçeve olan ISO 27001/27002, sağlayıcıların uymaları için daha iyi standartlar sağlar. Bu sebeple, Bulut Güvenliği Birliği (CSA) ile birlikte çok sayıda sanallaştırma ve bulut güvenliği uzmanı, ISO denetimi ve bulut ortamındaki kontrollerin durumlarının raporlanması için 27001/27002 standartlarını benimsemekte ve bulut sağlayıcılarına bu konuda çağrıda bulunmaktadırlar (Shackleford, 2010).

R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı: Bulut bilişim altyapıları sanallaştırma teknolojileri yoluyla, aynı fiziksel kaynaktan birden fazla kullanıcının faydalanmasına imkân tanıyan mimariler sunarlar. Ancak aynı fiziksel kaynağı paylaşan müşterilerden herhangi biri kötü niyetli faaliyetlerde bulunursa, bu durum aynı kaynağı kullanan diğer müşterilerin, bulut üzerinden sundukları hizmetlerin güvenilirliğine ve dolayısıyla da, ilgili kuruluşun piyasadaki itibarına zarar verebilmektedir. Örneğin spam gönderme, port tarama veya bulut altyapısından kötü niyetli içeriğin sunumu; altyapıdaki saldırganın yanında ve diğer müşteriler de dâhil belli bir aralıktaki bütün IP adreslerinin engellenmesine veya komşu faaliyetleri nedeniyle ilgili ortak kaynakların kullanımının durdurulmasına (örneğin mahkeme kararı gibi) yol çabilir. Bu durum sebebiyle müşteri kuruluş, hizmet sunumunda bozulma ve veri kaybının yanı sıra, kamuoyu önünde itibar kaybı yaşayabilir.

**SAS 70 Denetim Standartları Tablosu: Yeminli Mali Müşavirler Amerikan Enstitüsü (AICPA) tarafından geliştirilen bir tanınmış denetim standardıdır.

3.4.2. Teknik Riskler ve Güvenlik Riskleri

R.8- Dış Kaynaklı Saldırılar: Bulut servis sağlayıcıları, çok sayıda iş alanına destek sağlamaları ve hizmetlerinin internet üzerinden kullanılabilir olması sebepleriyle, kendi web site portalları aracılığıyla saldırıya uğrama riski altındadırlar. Saldırganlar hedef açısından zengin ortamları tercih etme eğilimindedirler ve bulut servis sağlayıcıları kendi hizmet alanları içinde birden fazla hedefe konsantredirler. Servis sağlayıcıların web desteği ve bulut yönetim araçlarını; müşterilerine web portalı üzerinden normal iş modelinin bir parçası olarak erişilebilir yapması ve böylece de bu araçları saldırganların erişilebileceği şekilde bırakması, durumu daha kötü hale getirir (Mosher, 2011). Bu saldırılara DDOS ve EDOS başlıca örnekler olarak verilebilir.

DDoS saldırıları (Distributed Denial of Service attack), çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur ve bunlar genellikle bir veya birden fazla web sunucusudur. Burada amaç genelde çalışan sisteme ait kaynakları durdurma veya yavaşlatmadır.

EDoS saldırılarında ise müşteri kaynaklarının ekonomik etki yaratacak şekilde, kötü niyetli diğer kişiler tarafından kullanılması söz konusudur. Burada saldırgan kimlik hırsızlığı yöntemiyle, kendi kazancı veya ekonomik olarak müşteriye zarar vermek için müşterinin kaynaklarını kullanmaktadır. Bulut mimarilerinde eğer müşteri ücret ödediği kaynakların kullanımı ile ilgili etkili sınırlamalar koymazsa, kötü amaçlı eylemler yoluyla, kaynakları üzerinde beklenmedik yükler deneyimleyebilir. Burada saldırgan kamuya açık bir kanal yoluyla müşterinin kaynaklarını kullanır. Bu saldırılar mali kaynaklara zarar verebilir, müşterilerin iflasına veya ciddi bir ekonomik kayıplara uğramasına yol açabilirler.

R.9- Verilerin Güvensiz veya Etkisiz Silinmesi: Bir müşteri sağlayıcısını değiştirdiği zaman, sağlayıcının o müşteriye ayırdığı kaynaklar geri alınarak, fiziksel donanım yeniden başka müşterilere tahsis edilir. Ancak hizmeti sonlandırılan müşterinin verileri, hizmet seviye anlaşmasında veya güvenlik politikasında yer alsa dahi tam olarak silinemeyebilir. Burada tam veri silme ancak diğer istemcilere ait verileri barındıran

diskin yok edilmesiyle mümkün olacağından, uygulanabilir değildir. Bir bulut kaynağını silmek için bir istek yapıldığında, bu durum verilerin gerçekten silinmesiyle sonuçlanmayabilir ve veriler çeşitli yöntemlerle geri getirilebilirler. Gerçek veri silme gereksinimlerinde özel işlemler takip edilmelidir ancak bu işlemler sağlayıcının standart API'leri tarafından desteklenmiyor olabilir. Burada risk düzeyini minimize etmek için, veritabanında etkin bir şifreleme prosedürü uygulamak gerekmektedir.

R.10- Nakil Halindeki Veriyi Yakalama: Bulut bilişimin dağıtık mimari yapısı, geleneksel altyapılara göre çok daha fazla verinin aynı anda dolaşımda olmasını sağlar. Örneğin, bir web sunucusu üzerindeki aynı fotoğraf veya görüntü verileri çoklu fiziksel makineler, bulut altyapısı ve uzak web istemciler vb. arasında sürekli transfer edilirler. Bu transferler sırasında dinleme, sızdırma, iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme, yan kanal ve veri iletimi tekrarlama saldırıları olası tehditlerdir. Bu tehditlere ilişkin sağlayıcı bir gizlilik taahhüdü sunmuyor veya bu taahhüt müşterinin bulut dolaşımdaki gizli bilgilerinin korunmasını garanti etmiyorsa, bu durum müşteri açısından ciddi bir risk oluşturur.

R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş: Sağlayıcı personeli içindeki özellikle yüksek ayrıcalıklı rol sahibi kişilerce veya bu kişilerin erişim yetkilerini ele geçiren üçüncü taraflarca gerçekleştirilebilecek kötü niyetli faaliyetler; veri gizliliği, veri bütünlüğü, verinin ulaşılabilirliği, hizmet ve uygulamalarla ilgili her türlü bozulma, aksama ve kesinti ve bunlara bağlı olarak kuruluşun itibarı, müşteri güveni ve çalışanların deneyimleri üzerinde potansiyel kötü etkilere sahip olabilirler. Bulut mimarilerinde, son derece yüksek riskli bazı rollerin zorunlu olması nedeniyle; bu duruma özellikle önem verilmelidir. Bu tür rollere örnek olarak; sağlayıcı sistem yöneticileri, denetçileri ve saldırı tespit raporları ve olay müdahale ile ilgili yönetilen güvenlik hizmeti sağlayıcıları verilebilir. Bulut kullanımı arttıkça, bulut sağlayıcılarının çalışanları giderek suç çeteleri için hedef haline gelmektedir (Catteddu, 2009).

R.12- Kaynak Tükenmesi: Bulut bilişim hizmetlerinin talep üzerine self servis kaynak temini özelliği, müşterilerin kaynak taleplerinin düzgün bir biçimde tahmin ve optimize

edilemediği durumlarda; sağlayıcı alt yapılarında kaynak tükenmesi problemlerine sebebiyet verebilmektedir. Bulut altyapıları idealde sınırsız kaynak sunuyormuş izlenimi yaratsa da, kaynak miktarı talebe göre sağlayıcı tarafından kiralama yoluyla artırılıp azaltılan bir yapıdadır. Sağlayıcılar belli istatistiklere göre müşterilerinden gelebilecek kaynak talebini belirler ve temin ederler. Ancak bu istatistik modellemelerde meydana gelen hatalar, sağlayıcının gerekli kaynağı doğru şekilde belirlemesine engel olabilmekte ve dolayısıyla yetersiz altyapı yatırımı yapmasına ve müşterilerine yetersiz kaynak aktarmasına neden olabilmektedir. Söz konusu kaynak belirleme algoritmalarında meydana gelebilecek hatalar sağlayıcı tarafında; sunulan hizmetlerin düzgün kullanılamaması, hizmetlere erişimin sağlanamaması, ekonomik kayıplar ve itibar kayıpları ve ayrıca fazlaca kaynak öngörülmesi sonucu oluşabilecek aşırı büyük altyapılara sebebiyet verebilmektedir. Müşteri açısından bakıldığındaysa yine kendi servis ve uygulamalarının son kullanıcılar tarafından kullanılamaması ve buna bağlı olarak oluşacak ekonomik kayılar ve itibar kayıpları gündeme gelebilecektir.

R.13- Şifreleme: Bulut şifreleme müşterilerin verilerinin şifreli metinlere dönüşümüdür. Bu şifreleme, kurum içi şifreleme ile önemli bir fark hariç hemen hemen aynıdır. Bu fark, bulut müşterisinin şifreleme ve şifreleme anahtarı yönetimi için sağlayıcının politika ve prosedürleri hakkında bilgi edinmesi gereksinimidir. Servis sağlayıcının bulut şifreleme yeteneklerinin, barındırılan verinin hassasiyet seviyesi ile eşleşmesi gerekir.

Şifreleme fazla işlemci yükü tükettiğinden, birçok bulut sağlayıcısı veritabanı alanında şifre ve hesap numaraları gibi sadece temel şifreleme hizmeti sunarlar. Bu noktada, bir sağlayıcının müşterisinin sahip olduğu tüm veritabanını şifrelemesi o kadar pahalı olabilir ki, müşterinin verilerini kurum içinde saklaması veya buluta göndermeden önce şifrelemesi daha mantıklı olabilir. Maliyetleri düşük tutmak için, bazı bulut sağlayıcıları fazla işlem gücü gerektirmeyen şifreleme alternatifleri sunmaktadırlar. Bu teknikler gizli veya sağlayıcı tarafından oluşturulan özel şifreleme algoritmaları kullanan, veri gözden geçirme ve gizleme prosedürleri içerir (Rouse, 2014a).

R.14- Kaynak İzolasyonu Eksikliği: Çok kiracılık ve işbirliği bulut bilişimin özünde var olan iki özelliktir. Kaynak izolasyonu eksikliği, aynı bulutun farklı istemcileri arasında ortak kullanılan depolama, bellek, yönlendirme vb. kaynaklarda meydana gelir. Ancak bu mekanizmalara yönelik saldırılar, geleneksel işletim sistemlerinde yaşanan saldırıları girişimleri kadar yaygın değildir ve teşebbüs edilmesi çok daha zordur (Jackson, 2011).

Eğer sağlayıcı hizmeti düzgün şekilde yapılandırılmamışsa, hizmet temel veri mimarisi, kuruluşun verilerinin diğer kuruluşlara ifşa edilmesi veya altyapıyı kullanan bir başka müşterinin, kuruluşun verilerine saldırması risklerini taşır. Bu saldırılara örnek olarak konuk atlamalı saldırılar, aynı tabloda depolanan birden fazla müşterinin verilerini teşhir eden SQL enjeksiyon saldırıları ve yan kanal saldırıları verilebilir. Bulut sağlayıcılar ve müşterileri için değerli veya hassas verilerin kaybı, itibar zedelenmesi ve hizmet kesintisi gibi olumsuzluklar yaratabilecek bu saldırılar; özel bulut mimarilerinde daha düşük oranda görülürken, açık bulutlarda göreceli olarak daha fazla görülmektedirler.

R.15- Hizmet Kesintisi veya Bozulması: Bulut sağlayıcıları internet üzerinden sundukları harici hizmetlerin herhangi bir bölümünde çeşitli sebeplerle tıkanıklık ve kesintiler yaşayabilirler. Bu sebeplere, sağlayıcıya kendi iç organizasyonundan veya dışarıdan yapılan bir saldırı nedeniyle kaynakların kullanılamaması, telekomünikasyon hatlarında tıkanıklıklar, başarılı bir sızma nedeniyle hizmetin kendisinin diğer hizmetlere yapılan saldırılar için üs olarak kullanılması ve diğer kötü niyetli saldırılar örnek olarak verilebilir. Yine benzer sebeplerle, bilinen tüm servis sağlayıcıları periyodik olarak hizmet dışı kalmalara ve performans sorunlarına maruz kalır.

R.16- Kötü Amaçlı Araştırma veya Taramalara Girişilmesi: Kötü amaçlı tarama, hedef bir makine veya ağ hakkında, ona karşı yapılacak saldırıyı kolaylaştırmak için bilgi toplama amacıyla kullanılan bir keşif tekniğidir. Hangi portların açık olduğunu keşfetmek, hangi hizmetlerin çalıştığını ve sistem yazılımını belirlemek için saldırganlar

tarafından kullanılan tarama; bir hedef makine içindeki güvenlik açıklarını tespit ve istismar için saldırganlara kolaylık sağlamaktadır (Kerr, 2001).

Zararlı tarama ve araştırmalar ve aynı zamanda ağ haritalama; bilgi toplama için kullanıldıklarından, bilişim varlıkları için dolaylı tehditler olarak kabul edilebilirler. Ancak sonuç olarak sunulan hizmet ve verinin gizlilik, bütünlük ve kullanılabilirliğinin kaybına sebep olabilirler.

R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık: Bulut sağlayıcıları, müşterilerinin üstlenmek zorunda olduğu asgari görevleri dile getirerek, sorumlulukları için açık bir bildirim ortaya koymalıdır. Bulut sağlayıcı, eğer müşteri izolasyonunu sağlamak için gerekli adımları atmamışsa, müşterilerinin bulut ortamının güvenliğini düzgün şekilde koruma konusundaki başarısızlıkları, tüm bulut platformu için de bir zafiyet teşkil edebilir. Bulut sağlayıcıları izolasyon mekanizmalarını daha fazla ortaya koymalı ve müşterilerine kaynaklarını korumada yardımcı olmak için en iyi uygulama yöntemlerini sağlamalıdır. Bazı durumlarda bulut müşterileri kendi veri güvenliğini sağlamak için gerekli tüm faaliyetlerden bulut sağlayıcının sorumlu olduğunu ve ilgili prosedürleri yürüttüğünü varsayarlar. Müşterinin bu varsayımı veya bulut sağlayıcısı tarafından kendisinin sorumlu olduğu prosedürlerin açıkça ortaya konulmaması durumu, verileri üzerinde gereksiz risk oluşturur. Bulut müşterilerinin kendi sorumluluklarını belirlemesi ve bunlara uyması şarttır.

İşin doğası gereği bulut sağlayıcıları, ister bir sunucu üzerinde sanallaştırma yoluyla olsun, isterse müşteriler tarafından paylaşılan ortak bir ağla olsun, çok kiracılı ortam sağlamakla yükümlüdürler. Birçok müşterinin ortak kullanımı, müşterilerin iletişim güvenlik gereksinimleri muhtemelen birbirinden farklı olacağından; kaçınılmaz olarak çatışmaya neden olur. Örneğin paylaşılan geleneksel ağ altyapısını üzerindeki iki müşteriden biri *SSH hariç tüm trafiği engellemek için ağ güvenlik duvarı isterken; bir web sunucusu çiftliği çalıştıran başka bir müşteri HTTP ve HTTPS geçişine ihtiyaç duyabilir. Bu durumda iki müşterinin ihtiyaçları ve güvenlik gereksinimleri arasında bir

* SSH (Secure Shell): Güvenli veri iletimi için kriptografik ağ protokolüdür.

uzlaşmazlık ortaya çıkar ve sağlayıcının iki müşteriyi aynı ortamda barındırması imkânsız hale gelebilir. Bu aynı tip sorunlar, uyumluluk gereksinimleri sebebiyle birbiriyle çelişen müşteriler tarafından ortaya atılabilir. Müşterilerin sayısındaki ve gereksinimlerinin farklılığındaki artış, bu durumu daha da kötü hale getirir. Bu nedenle, bulut sağlayıcıları teknoloji, politika ve şeffaflık yoluyla bu zorluklarla başa çıkabilecek kapasitede olmalıdırlar (Catteddu, 2009).

R.18- Şifreleme Anahtarlarının Kaybı: Güçlü şifreleme, hassas verileri korumak için merkezi ve temel bir savunmadır. Veri şifreleme süreci zor ve araçları karmaşık bir süreç değildir. Ancak, yaşam döngüleri boyunca çok sayıda ve sürekli değişen şifreleme anahtarlarını yönetmenin zorlukları ve güvenlik açıkları bulunmaktadır. Her şifreli verinin kendi kişisel anahtarının bulunması sebebiyle, binlerce şifreleme anahtarının yönetimi ve korunması kuruluş için büyük bir girişimdir. Kuruluşların veri güvenliğini sağlamak ve erişimi yönetilebilir kılmak için, piyasa rekabet gereksinimlerini dengelemeleri gerekir. Veri şifreleme anahtarlarının kaybı, şifrelenen verileri erişilemez ve karşılanamaz hale getirebilir. Kayıp bir şifreleme anahtarı, arızalı bir sabit sürücü veya bozuk bir veritabanı düzeyinde bir felakete yol açabilir (Advance Software Products Group, 2013).

Bu duruma örnek olarak; SSL, dosya şifreleme, müşteri özel anahtarları, vb. gizli anahtarların açığa çıkması, şifrelerin kötü niyetli kişilerin eline geçmesi, şifrelerin kaybı veya bozulması veya bunların kimlik doğrulama için izinsiz kullanılması verilebilir.

R.19- Hizmet Motorunun Hacklenmesi: Her bulut mimarisi, fiziksel donanım kaynakları üzerinde çalışan ve müşteri kaynaklarını farklı veri soyutlama düzeylerinde yöneten, son derece uzmanlaşmış bir platform olan hizmet motoruna dayanır. Örneğin, Servis olarak Altyapı (IaaS) servislerinde, bu yazılım bileşeni hipervizördür. Hizmet motorları, bulut platformu sağlayıcıları ve bazı durumlarda açık kaynak topluluğu tarafından geliştirilir ve desteklenirler. Her yazılım tabakası gibi, hizmet motoru kodunun da açıkları olabilir ve saldırılara veya beklenmeyen hatalara eğilimli olabilir. Saldırgan hizmet motorunu, bir sanal makine (IaaS bulut servisleri), çalıştırma ortamı

(PaaS bulut servisleri), uygulama havuzu (SaaS bulut servisleri) veya API'leri aracılığıyla hackleyerek tehlikeye atabilir. Servis motorunun hacklenmesi, farklı müşteri ortamları arasındaki izolasyondan kurtularak, bu ortamlar içinde bulunan verilere erişim sağlamak ve bu verileri kolay bir şekilde izlemek veya değiştirmek için; hizmet dışı bırakmaya neden olacak şekilde, aktarılan kaynakların azaltılmasına neden olmak şeklinde kullanılabilir (Catteddu, 2009).

3.4.3. Hukuksal Riskler

R.20- Yargı Değişiminden Kaynaklanan Riskler: Bir müşteri kuruluşun verilerinden bazıları, yüksek risk taşıyabilecek şekilde; birden fazla yargılamaya maruz kalabilir. Bulut sağlayıcıların kazanç, verimlilik ve güvenliklerini artırmak için; müşterilerinin verilerini farklı hukuk sistemlerinin geçerli olduğu farklı ülke veya bölgelerde barındırmaları, bu verilerle ilgili hukuki kararlar alınmasında zorluklara sebep olur. Örneğin, adli bir soruşturma için herhangi bir kurumunun bir bulut sağlayıcının altyapısında barındırdığı verilere ihtiyaç duyulması halinde; eğer bu veriler veri gizliliği yasa ve prosedürlerinin çok katı olduğu başka bir ülkede barındırılıyorsa ve fiziksel olarak diğer müşteri verileriyle aynı ortamda tutuluyorsa, ilgili verilerin tutulduğu ülkeden alınması o ülkenin yasalarına göre uygun değildir. Yine barındırılan verilerle ilgili bir ülkede suç teşkil eden bir durum, diğer bir ülkede serbest olabilir.

Yine veri merkezleri otokratik polis devletleri gibi; hukukun üstünlüğünün eksik olduğu, öngörülemeyen yasal çerçeve ve uygulanmalara sahip, uluslararası anlaşmalara saygı göstermeyen vb. yüksek riskli ülkelerde yer alıyorsa; veri merkezleri yerel yetkililer tarafından basılabilir ve sağlayıcılar bilgi, veri ve sistemlerini açıklamak veya el konulmasına izin vermek zorunda bırakılabilirler. Bu örnek tüm mahkeme celbi ve kolluk tedbirlerinin kabul edilemez olduğu anlamına gelmez. Ancak bazıları bu şekilde olabilir ve yine donanıma bazı meşru el koyma durumları da verilerin nasıl saklandığı bağlı olarak müşterileri olumsuz yönde etkileyebilir.

R.21- Mahkeme Celbi ve E-Keşif: Bir kuruluşun veri kaynaklarını tanımlaması, kaynaklar tamamen kendi kontrolü altında olsa bile yeterince zordur. Veri, bulut

sağlayıcının altyapısına aktarıldığında, eğer açık bir anlaşma ve tanımlama bulunmuyorsa; kuruluşun verinin tam nerede tutulduğu, kaç kopyasının bulunduğu ve ne şekilde düzenlendiği ile ilgili hiçbir bilgisi olmayabilir. Muhtemel bir e-keşifte mahkemelerin, kuruluşların verilerinin erişilebilir olmadığına dair açıklamalarını kabul etmesi olası değildir.

Kuruluşların veri barındırma politikaları, verilerin ömrünü kapsayacak şekilde oluşturulmalıdır. Konumu veya durumu ne olursa olsun; sıradan bir iş için veya keşif ile ilgili verilere erişimin gerekebileceği unutulmamalıdır. Bulut sağlayıcıların, verilerin periyodik olarak silinmesi ile ilgili kendi politikaları olabilir. Bu sebeple hizmet seviye anlaşması oluşturulurken; kayıt yönetimi, saklama protokolleri ve verilerin tutulma biçimi gibi konuları öngören durumlar için müzakere etmek kritik bir öneme sahiptir.

Müşteriler için, teknik konuların yanında, bulut sağlayıcıların ülke yetki alanı dışında veri depolaması ile ilgili büyüyen yasal endişeler vardır. Örneğin, maliyet, güvenlik veya başka nedenlerle bulut sağlayıcıları AB'de bilgi depolamayı tercih ederlerse, ABD e-keşif yükümlülüklerini hiç hesaba katmayan bu durum, bu ülkenin veri koruma yasalarını tetikleyebilir (Dale, 2012).

Ayrıca, kolluk kuvvetleri veya sivil görevliler tarafından mahkeme celbi sonucu fiziksel donanıma el konulması durumunda; fiziksel donanımdaki paylaşılan kiracılık durumu, yasal durumla ilgisi olmasa dahi çok daha fazla müşteriyi, istenmeyen taraflara verilerinin açıklanması riskiyle karşı karşıya getirir.

R.22- Veri Sansürü: Bazı durumlarda bulut sağlayıcıları, müşterileri tarafından hizmete sunulan herhangi bir veriyi, denetleme ve sansürleme hakkını saklı tutarlar. Bu durum, veri gönderme sürecinde gecikmelere veya verinin kendisinde kabul edilemez değişikliklere neden olabilir.

R.23- Lisans Riskleri: Bilgisayar başına anlaşmalar ve çevrimiçi lisans kontrolleri gibi lisans şartları, bulut ortamında işlemez hale gelebilir. Örneğin, eğer bir yazılım durum bazında ücretlendirilmişse, yeni bir makine aktif hale geldiğinde, aynı süre içinde aynı

sayıda makine kullanıyor olsa bile bulut müşterisinin lisanslama maliyetleri katlanarak artabilir. Servis olarak Platform (PaaS) ve Servis olarak Altyapı (IaaS) durumlarında bulut içinde özgün çalışmalar yaratma olasılığı da vardır. Burada, tüm fikri mülkiyet hakları uygun sözleşme şartları ile korunmuyorsa, bu özgün çalışma risk altında olabilir (Catteddu, 2009).

R.24- Veri Koruma Riskleri: Bulut bilişim, müşterileri ve sağlayıcılar için birkaç veri koruma riski oluşturmaktadır. Bulut müşterisi için, bulut sağlayıcının yürüttüğü veri işlemeyi etkili bir şekilde kontrol etmek ve böylece verinin yasal bir şekilde ele alındığından emin olmak zor olabilir.

Bulut sağlayıcı, dış işlemci rolü gereği bu tür işlemler gerçekleştirebilse bile; bulut müşterisinin, kişisel verilerin işlenmesinden sorumlu ana kişi olduğunun açık olması gereklidir. Veri koruma yasaları ülkeden ülkeye değişir ve bu yasalara uyulmaması veri sağlayıcısı için idari, hukuki ve cezai yaptırımlara yol açabilir. Bu sorun, birden çok bulut arasında veri transferi halinde daha da kötüleşmektedir. Diğer yandan, bazı bulut sağlayıcıları yürüttükleri veri işleme işinden bilgi sağlarlar. Bazıları da kendi veri işleme sertifikasyon özetlerini, veri güvenliği faaliyetlerini ve yaptıkları veri kontrollerini sertifikasyon kontrolörlerine sunarlar. Bulut sağlayıcısı tarafından kontrolöre bildirilmeyen veri güvenliği ihlalleri olabilir. Bulut müşterisi, bulut sağlayıcısı tarafından işlenen verinin kontrolünü kaybedebilir ve bu sorun, birden çok veri transferi halinde artabilir (Catteddu, 2009).

3.4.4. Buluta Özgü Olmayan Diğer Riskler

Aşağıda yer alan riskler, bulut bilişime özgü olmayan fakat tipik bir bulut tabanlı sistemin riskilerini değerlendirirken dikkatle düşünülmesi gereken hususlardır. Bu risklere kısaca değinilecektir.

R.25- Ayrıcalık Yükseltme Olasılığı: Ayrıcalık yükseltme, normalde bir uygulama veya kullanıcıdan korunan kaynaklara erişim sağlamak için, bir işletim sistemi ya da yazılım uygulamasındaki bir hata, tasarım kusuru veya yapılandırma dikkatsizliğini istismar etme eylemidir. Bu istismar sonucu, uygulama geliştiricisi veya sistem

yöneticisi tarafından istenenden daha fazla ayrıcalığa sahip olan ve yetkisiz eylemleri gerçekleştirebilen bir uygulama ortaya çıkar. Ayrıcalık yükseltme, yatay ve dikey olmak üzere ikiye ayrılır. Dikey ayrıcalık yükseltmede, daha düşük ayrıcalıklı bir kullanıcı veya uygulama, daha yüksek ayrıcalıklı kullanıcılar veya uygulamalar için ayrılmış fonksiyonlara ya da içeriğe erişir. Yatay ayrıcalık yükseltmedeyse, normal bir kullanıcı, diğer normal kullanıcılar için ayrılmış fonksiyonlara ya da içeriğe erişir. Ayrıcalık yükseltme diğer bilişim mimarilerinde olduğu gibi, bulut mimarisinde de güvenlik ve veri gizliliği gereksinimlerini tehlikeye atarak önemli bir risk faktörü oluşturur.

R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması: Kötü niyetli aktörlerin bir fiziksel konuma erişmesi olasılığı çok düşüktür ancak böyle bir durumun meydana gelmesinin bulut sağlayıcı ve müşterilerine etkisi çok yüksek olabilir. Bu durum şirket itibarını ve tesislerinde barındırılan verileri etkileyebilir. Bu risk yetersiz fiziksel güvenlik prosedürleri nedeniyle ortaya çıkar.

R.27- Ağ Kesilmeleri: Ağda fiziksel sebepler, enerji kesintileri veya kötü niyetli aktiviteler sonucu yaşanan kesintilerdir. Belli bölgedeki müşterileri aynı anda etkileyeceğinden çok ciddi risk potansiyeli taşırlar.

R.28- Sosyal Mühendislik Saldırıları: Bilgi güvenliği bağlamında sosyal mühendislik, çeşitli eylemler gerçekleştirerek, gizli bilgileri ifşa için insanların psikolojilerinin manipülasyonu anlamına gelir. Bilgi toplama, dolandırıcılık veya sistem erişimi amacıyla, genellikle birçok adımda olan ve güven veren karmaşık bir sahtekârlık düzeni olarak, geleneksel dolandırıcılıklardan farklıdır (Anderson, 2008). Telefon, sesli yanıt sistemi veya e-posta yoluyla kimlik avlama en çok kullanılan yöntemlerden biridir. Bunun yanında başkalarının giriş kartlarını kullanarak veri merkezlerine girme, teknik destek için aradığını söyleyerek kuruluş personellerinin telefonlarını rastgele arama, virüs yüklenen flash bellek veya CD'leri çalışma ortamlarına bırakarak çalışanların bu aygıtları açmaya çalışırken bilgisayarlarına truva atı tipi virüsler yüklemesini yol açma veya bir senaryo uydurarak ve hedef kişileri ikna ederek normal şartlarda yapmayacakları hataları yaptırma konusunda üstlerinde baskı oluşturma gibi çok çeşitli

yöntemler kullanılmaktadır. Bu yöntemlerle sağlayıcı veya müşteri tarafındaki yetkili kişilerin bulut sistemlerine giriş şifreleri ele geçirilebilir ve müşteri veya müşterilerin veri ve uygulamalarına izinsiz erişim sağlanabilir. Bu durum, hem veri gizliliği ve güvenlik taahütleri nedeniyle sağlayıcı ve hem de gizli bilgilerinin ifşası veya çalınması durumuyla karşı karşıya gelen müşteri açısında önemli bir risk oluşturur.

R.29- Hizmet Ücreti Değişikliği: Herhangi bir dış hizmette olduğu gibi, bulut hizmetlerinin de maliyetleri zamanla değişecektir. Bu tür değişiklikler hizmeti daha az maliyet etkin yapabilir ve hizmetin ilk etaptaki kullanılma amacını tehlikeye sokabilir.

R.30- Ağ Trafiğini Değiştirme: Bulut modellerinde ağdan ne tip ve boyutta veri aktarıldığına bağlı olarak, ağ trafiğinde değişimler meydana gelmektedir. Altyapıdaki sanallaştırma düzeyi ve sunucuların esnek bir şekilde farklı hizmetler sunmak üzere yeniden yapılandırılabilmesi, ağdaki veri aktarımını etkileyecektir. Yine yoğun veri analizi, paralel ve küme işleme, teletıp vb. yeni uygulamalar veri trafiğini önemli düzeyde artırırlar. Ayrıca uygulamalara mobil erişim gibi yeni erişim modelleri, sunucudan sunucuya trafik modelleri ve lokasyon bağımsız son kullanıcı erişimi ağ trafiğinde önemli değişikliklere sebep olurlar. Ancak altyapıda, uygulamalarda, erişimde ve ağ trafiği modelinde yaşanan bu değişikliklerle birlikte, verinin ağ üzerinden kullanılabilir şekilde akışını idame etmek gerekmektedir. Yine doğru kullanıcı, cihaz ve sistemlerin doğru zamanda doğru verilere erişimini temin etmek ve bu verileri saldırılara, ihlallere ve sızıntılara karşı korumak için, güvenlik prosedürleri etkili şekilde uygulanmaya devam etmelidir. Fakat farklı tipteki veri ve trafik çeşitlerinin, bütün ağ boyunca servis kalitesini sürdürmek adına, karşılanması gereken farklı önem düzeyi ve ağ kaynağı ihtiyaçları bulunmaktadır (Cisco, 2015). Bütün bu ihtiyaçların gerekli seviyede karşılanması ile ilgili yaşanan zorluklar ve ağ trafiğini bu doğrultuda ayarlamanın güçlüğü önemli riskler ortaya çıkarmaktadır.

R.31- Yedeklerin Kaybolması veya Çalınması: Yetersiz fiziksel güvenlik prosedürleri, erişim yönetimi açıkları ve kullanıcı yeniden yapılandırma açıkları nedeniyle oluşan bu yüksek etkili risk; şirket itibarını, tüm yedeklenen verileri ve hizmet sunumunu etkiler.

R.32- Doğal Afetler: Bu risk, meydana gelmesi durumunda kuruluşlar üzerinde büyük etki yaratabilecek düzeyde olsa da, göz ardı edilen risklerden biridir. Bir kuruluşun kötü veya denenmemiş bir iş sürekliliği ve felaket kurtarma planı varsa veya bundan da yoksunsa; itibarı, veri ve hizmet sunumu ciddi şekilde tehlikeye girebilir.

R.33- Ağ Yönetimi Sorunları: Bu tip sorunlara ağ tıkanıklığı, bağlantı sağlanamaması veya optimum olmayan kullanımlar sebebiyle sıkça ratlanır. Ağ tıkanıklığı, bir ağ devresinin kaldırabileceğinden daha fazla veri taşıması sonucu oluşur ve hizmetin kalitesinin düşmesine sebep olur. Tipik etkilere kuyruk gecikmesi, paket kaybı ya da yeni bağlantıların engellenmesi örnek olarak verilebilir. Yine ağın çeşitli sebeplerle aşırı şekilde yüklenmesi, bağlantı problemlerine neden olur ve hizmetelere erişimi engeller.

R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması: Operasyonel veya güvenlikle ilgili log kayıtları, politika eksikliği veya log toplamaya yönelik yanlış usuller nedeniyle kaybolabilir veya bozulabilirler. Bu durum aynı zamanda saklama ve erişim yönetimi açıkları, kullanıcı yeniden yapılandırma açıkları, yasal mevzuat eksikliği ve işletim sistemi açıkları nedeniyle meydana gelebilir.

3.5. Bulut Bilişimde Risk Olasılık Değerlendirmesi

Risk analizinde, bir riskin gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm riskler için olasılık değerlendirmesi yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, riskin cinsi, mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulmalıdır. Aşağıdaki tablo, ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi Standardı ve yine TS ISO 31000 Risk Yönetimi Standardı ile uyumlu şekilde, risk olasılıklarının değerlendirilmesi için beş kademeli bir çerçeve sunmakta olup; bir önceki alt bölümde belirlenen risklerin olasılıkları sırasıyla tablodaki değerlendirme koşulları göz önünde bulundurularak belirlenecektir.

Skor	Olasılık Derecesi	Değerlendirme	Olasılık	Sıklık
5	Beklenen	Riske bağlı olayın veya durumun meydana gelmesi kesindir veya olay son 6 ay içinde meydana gelmiştir.	% 90-100	Hemen her çeyrekte
4	Büyük İhtimalle	Riske bağlı olay veya durumun meydana gelmesi kuvvetle muhtemeldir.	% 70-90	Yılda bir
3	Olası	Riske bağlı olay veya durumun meydana gelmesi olasıdır.	% 50-70	2-4 yılda bir
2	Az Olası	Riske bağlı olay veya durumun meydana gelmesi az bir olasılıktır.	% 10-50	4-6 yılda bir
1	Çok Düşük Olasılık	Riske bağlı olay veya durumun meydana gelmesi çok düşük bir olasılıktır.	% < 10	7 yılda bir veya daha seyrek

Tablo 3.3: Risk Olasılıkları (Kaynak: Stone, 2016)

Bulut bilişim teknolojilerinde ortaya çıkan başlıca risklerin olasılık derecelerini sırayla değerlendirirsek:

R.1- Yönetim ve Kontrol Kaybı: Bu risk, veri ve uygulamaları için bir sağlayıcıdan hizmet alan veya ilgili sağlayıcının uygulamalarını kullanan müşterilerin hepsinde, kullandıkları hizmetin türüne göre değişse bile sıkça görülmekte olup, bu sebeple sürekli beklenen (5) bir risk olarak derecelendirilmektedir.

R.2- Bulut Hizmeti Sonlandırması veya Arızası: Sağlayıcının bulut hizmetini sonlandırması veya sürekli bir arıza sebebiyle uzun süreli hizmet kesintisi, çok az örneği olan bir durum olup; çok düşük olasılığa (1) sahip bir risk oluşturmaktadır.

R.3- Servis Sağlayıcı Bağımlılığı: Günümüzde birçok sağlayıcı, müşterilerin esnek bir şekilde bulut hizmeti aldığı sağlayıcıyı değiştirebilmesine engel olmak için, bulut uygulama ve API'lerinde standartlaşmaya karşı direnmektedir. Bu sebeple özellikle açık bulut ve topluluk bulutu kullanan kulanıcılar büyük ihtimalle (4) bu riskle karşılacaklardır.

R.4- Üçüncü Parti Tedarikçi Hatası: Bulut sağlayıcıların alt yüklenici altyapılarında meydana gelen hatalar dolayısıyla hizmet zincirinin bozulması durumuna, sağlayıcılarla tedarikçileri arasındaki bağlayıcı sözleşmeler ve sağlayıcıların böyle bir durumda hizmeti kısa sürede başka bir altyapı üzerinden devam ettirebilme esnekliğine sahip

olması sebepleriye sık rastlanmaz. Bunun için bu riskin meydana gelme olasılığı çok düşüktür (1).

R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması: Şirket satın alma her ne kadar ticari olarak sık karşılaşılabilecek bir durum olsa da, bulut sağlayıcı şirketlerin el değiştirmesi sık görülen bir durum değildir. Bu sebeple bu risk olası (3) olarak değerlendirilebilecektir.

R.6- Uyum Sorunları: Bulut teknolojileriyle ilgili standartların ülkesel ve küresel bazda halen geliştirilememiş olması, bu riskin sürekli beklenen (5) bir risk olmasına sebep olmaktadır.

R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı: Sağlayıcının diğer müşterilerinin kötü amaçlı veya diğer faaliyetleri sebebiyle, müşteri kuruluşun zarar görmesi, sağlayıcıların güvenlik, sunucu bölümlendirme ve izolasyon çalışmaları sonucu olasılığı az (2) bir risk haline gelmiştir.

R.8- Dış Kaynaklı Saldırılar: Gelişen filtreleme, olay yönetimi ve virüs koruma yazılımları dış kaynaklı saldırı olasılığını düşürmüştür. Bulut mimarileri dış kaynaklı saldırılara karşı topyekün bir şekilde, geleneksel mimarilere göre daha fazla mali kaynak aktarılmış güçlü güvenlik prosdürleri içerdiğinden, bu risk nedeniyle mimarinin zarara uğraması çok olası değildir (2). Ancak müşteri istemcileri tarafında, güvenlik bulut mimarisi kadar kompleks olmadığından, bu saldırıların başarıya ulaşma olasılığı artar.

R.9- Verilerin Güvensiz veya Etkisiz Silinmesi: Hizmet seviye anlaşmasının sona ermesi veya sağlayıcının hizmetlerini durdurması sebepleriyle müşteriyle ticari bağlantısının kesilmesi durumunda, müşteri verilerinin bir daha ulaşılamayacak şekilde silinmemesi, eğer buna zorlayacak cezai bir şart konulmamışsa olası (3) bir risktir.

R.10- Nakil Halindeki Veriyi Yakalama: Müşterilerin buluta aktardığı veya bulut altyapısından istemcilerine nakledilen verilerin kötü amaçlı olarak ele geçirilmesi, geleneksel bilişim mimarilerinde olduğu gibi bulut mimarilerinde de olası (3) bir risktir.

R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş: Günümüzde her ne kadar personel güvenlik soruşturmaları ve sabıka kaydı taramaları önem kazandıysa da, bulut sağlayıcı personelinin müşteri verilerine kötü amaçlı erişim sağlaması ve verileri ifşa edebilmesi olası (3) bir durumdur.

R.12- Kaynak Tükenmesi: Burada eğer sağlayıcı ile müşteri arasındaki hizmet seviye anlaşmasında, sağlanacak kaynağın miktarı belirtilmişse, hizmet sırasında kullanılan kaynağın yetersiz kalması riski düşüktür. Ancak bulut mimarilerinin birçoğunda bu tip bir kaynak miktarı öngörülmeden, talebe bağlı self-servis kaynak artırımı uygulandığından, risk olasılığı artmakta ve bu sebeple bu risk olası (3) olarak değerlendirilmektedir.

R.13- Şifreleme: Maliyeti artırması, arama ve aktarım süresini uzatması gibi nedenlerle, bulut altyapılarında yetersiz veri şifreleme algoritmalarının uygulanması durumu, sıkça rastlanan ve büyük ihtimalle (4) birçok sağlayıcıda görülebilecek bir durumdur.

R.14- Kaynak İzolasyonu Eksikliği: Sağlayıcı tarafından müşterilere sağlanan kaynak altyapısındaki izolasyon eksikliği sebebiyle, kullanıcıların birbirlerinin verilerini ve uygulamalarını etkileyebilmeleri durumu, çok sık rastlanan bir durum olmasa da, bu durum bulut mimarisine göre değişmektedir. Örneğin özel bulutlarda bu durum çok az görülürken, açık bulut mimarilerinde daha olasıdır. Burada kötü senaryo olan açık bulut mimarisi göz önünde bulundurularak risk olası (3) olarak değerlendirilecektir.

R.15- Hizmet Kesintisi veya Bozulması: Altyapı kaynakları ile ilgili teknolojik gelişmeler ve yedekleme stratejileri, gün geçtikçe bilişim hizmet kesintisi oran ve sürelerini azaltmaktadır. Ancak bulut bilişim gibi dağıtık, geniş, kontrolü zor ve pek çok farklı kaynaktan saldırıya maruz kalma olasılığı bulunan bir mimaride, genel veya lokal olarak hizmet kesintisi veya hizmetin kullanılabilirliğini kaybetmesi riskleri olası (3) durumlardır.

R.16- Kötü Amaçlı Araştırma veya Taramalara Girişilmesi: Ağ haritalama ve kötü amaçlı taramalar, geleneksel bilişim mimarileri kadar sık görülmese de, bulut mimarilerinde de olası (3) risk oluşturan tehditlerdir.

R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık: Segmentasyon, güvenlik prosedürleri, veri depolama yeri gibi konularda müşteri gereksinimleri ve sağlayıcı ortamı arasındaki uzlaşmazlık, her ne kadar hizmet seviye anlaşmasında bu unsurların açığa kavuşturulma seviyesine göre değişse de; pek sık rastlanılmayan, az olası (2) bir risktir.

R.18- Şifreleme Anahtarlarının Kaybı: SSL, dosya şifreleme veya müşteri özel şifrelerinin kaybı, sağlayıcının organizasyon yapısına göre firmadan firmaya değişişiklik gösterebilecekse de çok olası bir risk değildir (2).

R.19- Hizmet Motorunun Hacklenmesi: Fiziksel altyapının üzerinde bulunan ve farklı soyutlama düzeylerinde müşteri kaynaklarını yöneten hipervizör gibi hizmet motorlarının başarılı saldırılara uğraması, olasılığı düşük (2) bir risktir.

R.20- Yargı Değişiminden Kaynaklanan Riskler: Farklı ülke veya bölgelerdeki yargı mevzuatı nedeniyle müşteri ve sağlayıcı varlıklarının karşılaştığı bu riskler, sağlayıcıların maliyet, verimlilik ve güvenlik gibi kaygılarla, verileri farklı lokasyonlarda barındırma eğilimleri nedeniyle; çok yüksek olasılığa sahip, sürekli beklenen (5) riskler haline gelmektedir.

R.21- Mahkeme Celbi ve E-Keşif: Günümüzde bilişim suçlarının artması, veri sızdırma, veri ifşası, hizmet çökertme gibi birtakım kötü amaçlı faaliyetlere sıkça rastlanması ve ayrıca bulut müşterilerinin kendileri veya kullanıcıları hakkındaki yargılamalar sebebiyle ilgililerin verilerine yargı yoluyla el koyulması durumları, bu riskin olsılığını artırmaktadır. Bu sebeple bu risk büyük ihtimalle (4) asgari her yıl gerçekleşebilme olasılığı taşımaktadır.

R.22- Veri sansürü: Sağlayıcı tarafından müşteri verisinin sansürlenmesi veya denetlenmesi, eğer hizmet seviye anlaşmasında belirtilmemişse olası (3) bir durumdur.

R.23- Lisans Riskleri: Sanal makinelerde kullanılan yazılımların lisans ücretlerinin, bulut mimarisindeki sanal makinelerin dinamik bir şekilde oluşturulup kapatılabilmesi sebebiyle, müşteri açısından önemli maliyetlere ulaşabilmesi veya müşterinin bulut altyapısında kendi oluşturduğu yazılımların lisanslanmasıyla ilgili ortaya çıkabilecek bu riskler; bulut mimarileri için olası (3) risklerdir.

R.24- Veri Koruma Riskleri: Yargı mevzuatı değişimleri, sağlayıcı uygulamaları sebebiyle müşterinin veri kontrolünü kaybetmesi ve müşteriye bildirilmeyen veri güvenliği ihlalleri gibi nedenlerle; müşterilerin verilerinin koruması ile ilgili ortaya çıkan bu riskler, birçok bulut sağlayıcı hizmetinde büyük ihtimalle (4) rastlanabilecek risklerdir.

R.25- Ayrıcalık Yükseltme Olasılığı: İster yatay isterse dikey yönde olsun; yanlış veya eksik yapılandırma ve rol atama ile hipervizör, erişim yetkilendirme ve şifre yönetimi açıkları sebebiyle, bazı kullanıcıların yetkilerinin artırılması riski bulut mimarilerinde olasığı az (2) bir durumdur.

R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması: Bu tip fiziksel erişim veya hırsızlık gibi eylemlerin görülme riski, alınan fiziksel güvenlik önlemleri sayesinde çok düşük (1) bir olasılıktır.

R.27- Ağ Kesilmeleri: Burada bahsedilen risk, bulut bilişim müşterilerinin istemci cihazlarının bağlı olduğu ağlardaki kesintilerde değil, sağlayıcının hizmet sunduğu ağda meydana gelebilecek kesintilerde ortaya çıkabilecektir. Sağlayıcıların farklı lokasyonlarda barındırma ve yedekleme stretejileri sayesinde, hizmet sundukları ağda kesintiler yaşanması çok olası değildir (2).

R.28- Sosyal Mühendislik Saldırıları: Sağlayıcı personelini kandırmak, yanlış yönlendirmek veya çeşitli kötü amaçlı yazılımlar kullanmak suretiyle; şifre ve bilgilerini ele geçirmeye dayalı bu saldırılar bulut mimarilerinde görülmesi olası (3) risklerdir.

R.29- Hizmet Ücreti Değişikliği: Sağlayıcıların, müşterilerinin kendisine bağımlılığından faydalanarak, hizmet seviye anlaşmalarındaki boşluklar veya seviye

anlaşması süresinin sona ermesi gibi durumlar nedeniyle, sağladığı hizmetin ücretlerinde değişikliğe gitmesi, bulut mimarilerinde olası (3) bir risktir.

R.30- Ağ Trafiğini Değiştirme: Saldırılar, platform değişiklikleri veya büyük veri aktarımı gerektiren uygulamaların kullanımında yaşanan ani artışlara bağlı olarak, ağın yeni veri trafiği yükünü kaldırılabilecek şekilde ayarlanması önündeki riskler, sağlayıcıların, sağladıkları hizmetlere göre yaptıkları istatiksel analizler sonucunda uyguladıkları ayarlama senaryoları sayesinde; çok rastlanmayan, az olası riskler (2) olarak değerlendirilecektir.

R.31- Yedeklerin Kaybolması veya Çalınması: Yine uygulamalar veya verilere ait yedeklerin kaybolması veya çalınması nadiren görülen, çok olası bir risk değildir (2).

R.32- Doğal Afetler: Bölgeden bölgeye değişiklik gösterebilmekle birlikte, yaşanabilecek doğal afetler nedeniyle fiziksel altyapının zarar görmesi çok düşük (1) bir olasılıktır.

R.33- Ağ Yönetimi Sorunları: Sağlayıcı tarafında yanlış yapılandırma, yazılım hataları, iş sürekliliği ve felaket kurtarma planlarının ve kaynak izolasyonunun eksikliği gibi nedenlerle; ağ yönetimini ve dolayısıyla hizmet kullanılabilirliğini etkileyebilecek tehditler olası (3) riskler oluşturur.

R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması: Bu tip log kayıtlarının, birçok bulut sağlayıcı ortamında yedekli olarak güvenli bir şekilde tutulması önem arz ettiğinden, risklerin olasılığı azdır (2).

3.6. Bulut Bilişimde Risk Etki Analizi

Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçeklenmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır. Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (ve sakladığı veya

işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir. Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır (Eskiyörük, 2007). Aşağıdaki tablo ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi Standardı ve yine TS ISO 31000 Risk Yönetimi Standardı ile uyumlu şekilde risk olasılıklarının değerlendirilmesi için beş kademeli bir çerçeve sunmakta olup; bir önceki alt bölümde belirlenen risklerin olasılıkları sırasıyla tablodaki değerlendirme koşulları göz önünde bulundurularak belirlenecektir.

Skor	Etki Derecesi	Tanım	Etki Süresi
5	Yıkıcı Etki	Kuruluşun varlıklarında veya itibarında şiddetli ve yıkıcı bir hasara neden olan, örneğin dışarıdan etkileri görünen ve kuruluş çalışmalarını ve vatandaşların güvenini etkileyen durumlardır.	Çok Uzun Düzelme Dönemi
4	Şiddetli Etki	Kuruluşun varlıklarında veya itibarında şiddetli ama yıkıcı olmayan bir hasara neden olan, örneğin dışarıdan görünen ve kuruluş çalışmalarını ve vatandaşların güvenini etkileyen durumlardır.	Uzun Düzelme Dönemi (12-24 ay)
3	Ciddi Etki	Orta hasar veya kayba neden olur, örneğin iç operasyon, operasyonel maliyetlerin artmasına veya hizmet seviye anlaşmasının performansının azalmasına neden olur.	Kısa Dönem Düzelme (6-12 ay)
2	Hafif Etki	Küçük bir hasar veya kayba neden olur, örneğin iç operasyonları etkiler ama maliyetlerindeki artış önemsizdir.	Geçici Etki (6 aydan az)
1	Düşük Etki	Varlıklarda küçük değişikliğe sebep olur veya hiçbir değişikliğe neden olmaz. Normal iş operasyonları tarafından emilir; maliyetler, verimlilik ve iş taahhütleri üzerinde ölçülebilir bir etki yaratmaz.	Minimal Etki

Tablo 3.4: Risk Etkileri (Kaynak: Stone, 2016)

R.1- Yönetim ve Kontrol Kaybı: Bu riskin gerçekleşmesi sonucu sağlayıcıya bağlı olarak müşteri kuruluşun veri ve uygulamaları kendi kontrolünden çıkıp sağlayıcının insiyatifine gireceğinden yıkıcı etkisi (5) olabilecek sonuçlar doğurabilir. Ancak risk

etkisi kullanılan servis modeline de bağlıdır. Örneğin Servis olarak Altyapı (IaaS) modelinde kuruluşun sağlayıcı altyapısına aktardığı veri ve uygulamaların hepsi tehlikeye gireceğinden yıkıcı, Servis olarak Yazılım (SaaS) modelinde ise yazılım, uygulama ve verilerin önemli bölümü zaten sağlayıcıya ait olduğundan hafif bir etki ortaya çıkacaktır. Bu risk için en kötü senaryo olan Servis olarak Altyapı (IaaS) modeli göz önünde bulundurulacaktır.

R.2- Bulut Hizmeti Sonlandırması veya Arızası: Sağlayıcının bulut hizmetini sonlandırması veya sürekli bir arıza sebebiyle müşterilerin uzun süreli hizmet kesintisi nedeniyle müşteri kuruluşun karşı karşıya kalacağı uzun süreli hizmet kesintisi; verimliliği, iç operasyonları, maliyetleri, iş taahhütleri gibi birçok konuda yıkıcı etkiler (5) oluşturmaktadır.

R.3- Servis Sağlayıcı Bağımlılığı: Müşterilerin esnek bir şekilde bulut hizmeti aldığı sağlayıcıyı değiştirememeleri, değiştirmeye çalıştıklarında uygulama yazılımlarını revize etmelerinin gerekmesi ve verilerini tam olarak geri alma konusunda yaşayabilecekleri sorunlar maliyet, iç operasyonlarının artmasına neden olabilecek ciddi bir etki (3) yaratır.

R.4- Üçüncü Parti Tedarikçi Hatası: Bulut sağlayıcıların alt yüklenici altyapılarında meydana gelen hatalar dolayısıyla hizmet zincirinin bozulması durumu; sağlayıcılar böyle bir duruma karşı hizmeti kısa sürede başka bir altyapı üzerinden devam ettirebilme esnekliğine sahip olsalar bile, müşteri kuruluşların iç operasyonlarını artırıp, hizmet seviye anlaşmasının uygulanması ile ilgili performası düşüreceğinden müşteri kuruluş açısından ciddi etkiler (3) oluşturabilir.

R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması: Sağlayıcı şirketlerin el değiştirmesi durumu, müşteri kuruluşun hizmetlerinde kesintiye sebep olabilir fakat genelde satın alan firmaların sağlayıcının ticari ünvanını değiştirmemesi ve müşterilerini kaybetmemek adına mevcut sözleşmelere sadık kalması nedeniyle bu risk ciddi etki (3) yaratabilecek bir risk olarak değerlendirilmektedir.

R.6- Uyum Sorunları: Bulut teknolojileriyle ilgili standartların ülkesel ve küresel bazda halen geliştirilememiş olması, denetimde ve standartlaşmada yaşanan sorunlar kuruluşun veri kaybına, veri güvenliğinin tehlikeye girmesine ve sonuç olarak maliyet, iç operasyonlarının artmasına ve kullanıcı vatandaşların güven kaybına neden olabilecek şiddetli etkiler (4) yaratabilir.

R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı: Sağlayıcının diğer müşterilerinin kötü amaçlı veya diğer faaliyetleri sebebiyle, müşteri kuruluşun itibar kaybı her ne kadar olasılığı az bir risk olsa da maliyet, vatandaşların güven kaybı nedeniyle iş verimliliği ve taahhütleri ile ilgili şiddetli etkiler (4) yaratabilir.

R.8- Dış Kaynaklı Saldırılar: Sağlayıcı altyapısına yönelik dış kaynaklı saldırıların başarılı olması, sağlayıcının bütün veya önemli sayıda müşterisinin verilerinin güvenliğini ve gizliliğini ortadan kaldıracağından birçok konuda yıkıcı etkiler (5) yaratacaktır.

R.9- Verilerin Güvensiz veya Etkisiz Silinmesi: Hizmet seviye anlaşmasının sona ermesi veya sağlayıcının hizmetlerini durdurması dolayısıyla müşteriyle ticari bağlantısının kesilmesi durumunda, müşteri verilerinin bir daha ulaşılamayacak şekilde silinmemesi, müşteri kuruluşun kendi iç personelinin ve hizmet kullanıcılarının tüm verilerinin ifşasına yol açabileceğinden iç operasyonları, maliyetleri, iş taahhütleri gibi birçok konuda yıkıcı etkiler (5) yaratabilecektir.

R.10- Nakil Halindeki Veriyi Yakalama: Müşterilerin buluta aktardığı veya bulut altyapısından istemcilerine nakledilen verilerin kötü amaçlı olarak ele geçirilmesi müşteri veri gizliliğini tehlikeye sokacak olup itibarı, iç operasyonları üzerinde şiddetli etkiler (4) oluşturabilir.

R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş: Bulut sağlayıcı personelinin müşteri verilerine kötü amaçlı erişim sağlaması ve verileri ifşa edebilmesi durumu, müşteri verilerinin güvenliğini ve gizliliğini tamamen ortadan kaldıracağından, müşteri

verimliliği, iç operasyonları, maliyetleri, iş taahhütleri gibi birçok konuda yıkıcı etkiler (5) yaratabilecektir.

R.12- Kaynak Tükenmesi: Burada eğer sağlayıcı ile müşteri arasındaki hizmet seviye anlaşmasında sağlanacak kaynağın miktarı belirtilmişse ve sağlayıcı bu kaynağı bile sağlayamıyorsa bu durum müşteri operasyonlarını tamamen durduracağından yıkıcı bir etki yaratabilir. Ancak bu tip bir kaynak miktarı öngörülmeden sadece sağlayıcı tarafından yapılan istatistiksel çalışmaya göre sağlanan kaynağın, müşterinin kendi servislerinin hizmet yükünün pik yaptığı zamanlarda talebi karşılamaması durumu, dönemsel bir durum olduğundan ancak ciddi bir etki (3) oluşturabilir. Burada risk olasılığı bölümünde ikinci durum göz önünde bulundurulduğundan, risk etkisi hesaplanırken yine ikinci durum değerlendirilmektedir.

R.13- Şifreleme: Maliyet ile arama aktarım süresini uzatması gibi nedenlerle bulut altyapılarında yetersiz veri şifreleme algoritmalarının uygulanması yine müşteri kuruluşun veri gizliliğini tehlikeye atacağından, itibarı ve iç operasyonları üzerinde şiddetli etkiler (4) oluşturabilir.

R.14- Kaynak İzolasyonu Eksikliği: Sağlayıcı tarafından müşterilere sağlanan kaynak altyapısındaki izolasyon eksikliği sebebiyle kullanıcıların birbirlerinin verilerini ve uygulamalarını etkileyebilmeleri durumu çok sık rastlanan bir durum olmasa da, böyle bir durumda müşteri verimliliği, iç operasyonları, maliyetleri, iş taahhütleri gibi birçok unsur kötü yönde etkileneceğinden yıkıcı (5) bir etki oluşturması beklenebilecektir.

R.15- Hizmet Kesintisi veya Bozulması: Altyapı kaynakları ile ilgili teknolojik gelişmeler ve yedekleme stratejileri gün geçtikçe bilişim hizmet kesintisi oran ve sürelerini azaltmaktadır. Ancak süresi ne olursa olsun hizmet kesintisi kuruluşun kamuoyu önündeki itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) bırakabilir.

R.16- Kötü Amaçlı Araştırma veya Taramalara Girişilmesi: Ağ haritalama ve kötü amaçlı taramaların, veri gizliliğinde bozulmaya ve müşterilerin kullandığı kaynakların bilgisayar korsanlarının hedefi haline gelmesine yol açabilecek ciddi etkileri (3) olabilir.

R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık: Segmentasyon, güvenlik prosedürleri, veri depolama yeri gibi konularda müşteri gereksinimleri ve sağlayıcı ortamı arasındaki uzlaşmazlık eğer ilgili konularda hizmet seviye anlaşmasında bir koşul belirtilmemişse, müşteri kuruluşların verimliliği ve iş taahhütleri üzerinde ciddi etkiler (3) oluşturabilir.

R.18- Şifreleme Anahtarlarının Kaybı: SSL, dosya şifreleme veya müşteri özel şifrelerinin kaybı her ne kadar çok sık ratlanan bir durum olmasa da bazı durumlarda müşteri verilerinin bozulması sonucunu doğuracağından müşterinin itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) bırakabilir.

R.19- Hizmet Motorunun Hacklenmesi: Fiziksel altyapının üzerinde bulunan ve farklı soyutlama düzeylerinde müşteri kaynaklarını yöneten hipervizör gibi hizmet motorlarının başarılı saldırılara uğraması olasılığı düşük olsa da, bu saldırılar bütün müşterilerin verilerinin güvenliğini ve gizliliğini ortadan kaldıracağından yıkıcı etkiler (5) yaratabilir.

R.20- Yargı Değişiminden Kaynaklanan Riskler: Farklı ülke veya bölgelerdeki yargı mevzuatı nedeniyle müşteri ve sağlayıcı varlıklarına ilgili ülke veya bölgenin yargısının geçici veya sürekli olarak el koyması olasılığı mevcuttur. Böyle bir durumun müşteri kuruluşun iç operasyonları, maliyetleri, iş taahhütleri gibi hususlar üzerinde şiddetli etkiler (4) yaratacağı açıktır.

R.21- Mahkeme Celbi ve E-Keşif: Günümüzde bilişim suçlarının artması, veri sızdırma, veri ifşası, hizmet çökertme vb. gibi birtakım kötü amaçlı faaliyetlere sıkça rastlanması ve ayrıca bulut müşterilerinin kendileri veya kullanıcıları hakkındaki yargılamalar dolayısıyla ilgililerin verilerine yargı yoluyla el koyulması durumları; el konulan verinin sadece yargı organlarının incelenmesi için alıkonulacağı ve bunun belli

bir süre sonra sona ereceği düşünüldüğünde verinin tamamen kaybolmasına veya ifşa olmasına yol açmaz. Ancak yine de müşterilerin kendi kullanıcılarına verecekleri hizmetlerin sekteye uğraması sebebiyle ciddi etkiler (3) yaratabilirler.

R.22- Veri sansürü: Sağlayıcının müşteri verisini sansürlenmesi veya denetlenmesi; kuruluşun kamuoyu önündeki itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) bırakabilir.

R.23- Lisans Riskleri: Sanal makinelerde kullanılan yazılımların lisans ücretlerinin, bulut mimarisinde sanal makinelerin dinamik bir şekilde oluşturulup kapatılabilmesi sebebiyle müşteri açısından önemli maliyetlere ulaşabilmesi veya müşterinin bulut altyapısında kendi oluşturduğu yazılımların lisanslanmasıyla ilgili ortaya çıkabilecek riskler sadece operasyonel maliyetleri ve verimliliği etkileyecek olsa da, yine de öngörülemeyen maliyetler ciddi etkiler (3) oluşturabilir.

R.24- Veri Koruma Riskleri: Yargı mevzuatı değişimleri, sağlayıcı uygulamaları sebebiyle müşterinin veri kontrolünü kaybetmesi ve müşteriye bildirilmeyen veri güvenliği ihlalleri gibi nedenlerle, veri güvenliğinin ve gizliliğinin uzun süreli tehlikeye girmesi riskleri, müşteri veri gizliliğini tehlikeye sokacak olup itibarı, iç operasyonları üzerinde şiddetli etkiler (4) oluşturabilir.

R.25- Ayrıcalık Yükseltme Olasılığı: Yatay veya dikey yönde yanlış veya eksik yapılandırma ve rol atama, hipervizör, erişim yetkilendirme ve şifre yönetimi açıkları sebebiyle bazı kullanıcıların yetkilerinin artırılması diğer müşterilerin veri gizliliğini tehlikeye sokacak olup; itibarları ve iç operasyonları üzerinde şiddetli etkiler (4) oluşturabilir.

R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması: Bu tip fiziksel erişim veya hırsızlık gibi eylemlerin görülme riski az olsa da müşterilerin veri gizliliği kaybolacağından, kuruluşun itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) yaratabilecektir.

R.27- Ağ Kesilmeleri: Sağlayıcının hizmet sunduğu ağda meydana gelebilecek kesintiler, müşteriye sunulan hizmetin tamamen kesilmesi sonucunu doğuracağından, iç operasyonları, maliyetleri, iş taahhütleri gibi birçok konuda yıkıcı etkiler (5) yaratabilecektir.

R.28- Sosyal Mühendislik Saldırıları: Sağlayıcı personelini kandırmak, yanlış yönlendirmek veya çeşitli kötü amaçlı yazılımlar kullanmak suretiyle şifre ve bilgilerini ele geçirme durumu kısa süreli de olsa, şifresi ele geçirilen kişinin yetki durumuna göre bir miktar veya tüm müşterilerin verilerinin gizliliğini ve güvenliğini tehlikeye atacağından şiddetli etkiler (4) yaratması beklenebilir.

R.29- Hizmet Ücreti Değişikliği: Sağlayıcıların, müşterilerinin kendisine bağımlılığından faydalanarak, hizmet seviye anlaşmalarındaki boşluklar veya seviye anlaşması süresinin sona ermesi gibi durumlar nedeniyle sağladığı hizmetin ücretlerinde değişikliğe gitmesi durumu müşterilerin sadece maliyetlerini etkileyeceğinden hafif bir etki (2) bırakması beklenebilir.

R.30- Ağ Trafiğini Değiştirme: Saldırılar, platform değişiklikleri veya büyük veri aktarımı gerektiren uygulamaların kullanımında yaşanan ani artışlara bağlı olarak ağın yeni veri trafiği yükünü kaldırılabilecek şekilde ayarlanması önündeki riskler hizmet kullanılabilirliğini geçici de olsa etkileyeceğinden, müşteri kuruluşun itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) yaratabilecektir.

R.31- Yedeklerin Kaybolması veya Çalınması: Uygulamalar veya verilere ait yedeklerin kaybolması veya çalınması durumunda hizmet kesintisi yaşanmayacak fakat müşteri verilerinin gizliliği ortadan kalkabilecektir. Bu sebeple şiddetli bir risk (4) oluşturması kaçınılmazdır.

R.32- Doğal Afetler: Yaşanabilecek doğal afetler nedeniyle fiziksel altyapının zarar görmesi durumu her ne kadar birçok bulut altyapısı yedekli olarak barındırılsa da, eğer yedekleme de sorunlar varsa ve yedekleme bu afetten ikisi de etkilenecek iki ayrı lokasyonda yapılıyorsa; geçici olarak hizmet kesintilerine sebeiyet verip müşteri

verilerinin kaybolmasına yol açabileceğinden; kuruluşun itibarı, iç operasyonları ve iş taahhütleri üzerinde şiddetli etkiler (4) yaratabilecektir.

R.33- Ağ Yönetimi Sorunları: Sağlayıcı tarafında yanlış yapılandırma, yazılım hataları, iş sürekliliği ve felaket kurtarma planlarının ve kaynak izolasyonunun eksikliği gibi nedenlerle ağı yönetimini ve dolayısıyla hizmet kullanılabilirliğini sürekli olarak etkileyebilecek tehditler; müşteri kuruluşun itibarı, maliyetleri, iç operasyonları ve iş taahhütleri üzerinde yıkıcı etkiler (5) oluşturabilecektir.

R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması: Bu tip log kayıtlarının birçok bulut sağlayıcı ortamında az görülen bir durum olsa da, müşterilerin iç operasyonları ve iş taahhütleri üzerinde ciddi etkiler (3) oluşturabilir.

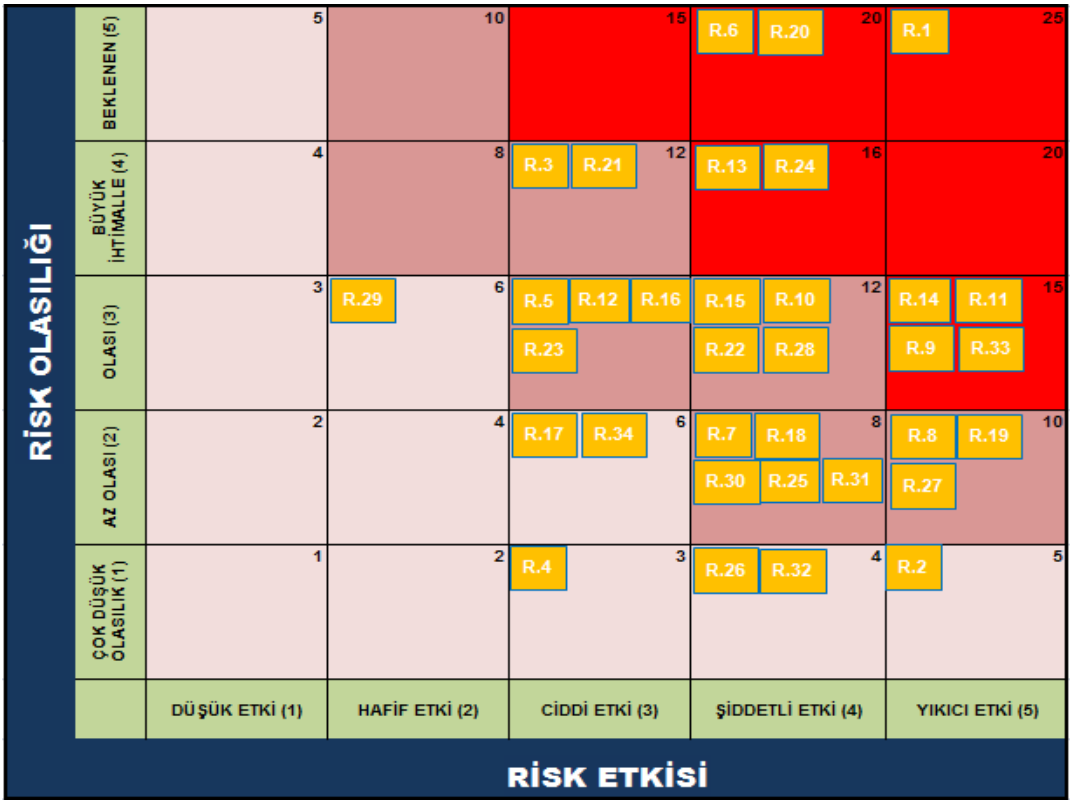
3.7. Bulut Bilişimde Risk Değerlerinin Bulunması

Risk değerlerinin bulunmasının amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır. Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır (Eskiyörük, 2007).

Dünyaca kabul görmüş risk analizi metodlarından iri olan ISRAM Türkiye Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü ve Gebze Teknoloji Enstitüsü'nde Aralık 2003'te geliştirilmiştir. Bu metod risk analizine kuruluşun yönetim ve personelinin katılımına olanak sağlayan kantitatif bir yaklaşım getirmektedir. ISRAM modelinde genel risk formülü temel alınmıştır. Bu formül, Risk = Güvenlik ihlalinin olma olasılığı x ihlalin yapacağı etki şeklindedir. Yine web uygulama güvenliği alanında açık kaynaklı makaleler, metodolojiler, belgeler, araçlar ve teknolojiler geliştiren ve online bir topluluk olan OWASP'ın gelişirdiği ve OWASP risk derecelendirme metodolojisinde Risk Değeri = Olasılık x Etki olarak hesaplanmaktadır. Bu metodlar

ışığında bu çalışmada risk değerlerinin hesaplanmasında, Risk Değeri= Risk Olasılığı x Risk Etkisi formülü kullanılmıştır.

Aşağıda önceki bölümlerde bulunan risk olasılığı ve risk etkisi değer çiftleri için; düşük, orta ve yüksek olmak üzere üç seviyeli risk derecelendirme matrisi oluşturulmuştur. Bu matriste açık pembeyle vurgulanan bölümler risk olasılığı ve risk etkisi çarpımının 7'den küçük olduğu bölümler olup, düşük risk seviyesini temsil etmektedirler. Buna göre 2,4,17,26,29,32,34 numaralı riskler düşük seviyeli riskler olarak değerlendirilmiştir. Yine koyu pembeyle vurgulanan bölümler risk olasılığı ve risk etkisi çarpımının 7'den büyük ve 15'ten küçük bölümler olup, orta risk seviyesini temsil etmektedir. Buna göre 3,5,7,8,10,12, 15,16,18,19,21,22,23,25,27,28,30,31 numaralı riskler orta seviyeli riskler olarak değerlendirilmiştir. Son olarak kırmızıyla vurgulanan bölümler risk olasılığı ve risk etkisi çarpımının 15'ten büyük olduğu bölümler olup, yüksek risk seviyesini temsil etmektedirler. Buna göre 1,6,9,11,13,14,20,24,33 numaralı riskler yüksek seviyeli riskler olarak değerlendirilmiştir.



Tablo 3.5: Risk Derecelendirme Matrisi

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçeklenmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir. Yukarıdaki risk derecelendirme matrisinde belirtilen farklı renklere göre risk seviyesi tanımlarına ve açıklamalarına aşağıdaki tabloda yer verilmiştir.

Risk derecesi	Risk açıklaması ve yapılması gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içersinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Tablo 3.6: Risk Dereceleri ve Tanımları (Kaynak: Eskiyörük, 2007).

4. KAMUDA BULUT BİLİŞİM RİSK YÖNETİMİ

Risk yönetimi, kuruluşların başına gelmesini istemediği olaylar için; bu olaylara yol açabilecek riskleri belirlemek, değerlendirmek ve azaltmak için kullanabileceği bir süreçtir. Bu bağlamda kuruluşların faaliyet alanları belirlenerek; bu alanlardaki muhtemel riskleri bu yönetim süreci metodolojisi kullanılara işlenir ve böylece kuruluşun performansını artırma ve rekabet gücünü üst düzeyde tutma amaçlanır. Bu yönetim modeli riski tespit etmeye, değerlendirmeye, kesin ve sürekli olarak onu kontrol etmeye yarayan temel yapıları içinde barındırmaktadır. Risk yönetimi süreçleri, finansal piyasalar, proje yönetimi, mühendislik, endüstriyel prosesler, kamu sağlığı, güvenliği ve emniyeti gibi birçok alanda takip edilebilir. Ancak, risk yönetimi yöntemleri, tanımları ve hedefleri kullanılacağı alana göre değişiklik gösterebilecektir. Örneğin bilgi güvenliği risk yönetimi süregelen bir faaliyet olup, bu faaliyette, güvenlik politikası, antivirüs, güvenlik duvarı vb. güvenlik mekanizmaları düzenli olarak takip edilmeli ve doğru ve etkili bir şekilde çalışabilmelerini sağlamak için gözden geçirilmelidirler. Bu süreçte log kayıtlarının günlük kontrolü gibi güvenlik mekanizmalarının çoğu doğru ve uygun işleyişini sürdürebilmek için, bakım ve idari destek gerektirecektir. Ayrıca, özgün güvenlik risk değerlendirmesi ve yönetimi sonuçlarının da, meydana gelebilecek değişiklikler göz önünde bulundurularak düzenli olarak gözden geçirilmesi gerekmektedir. Başlangıçta değerlendirilen risklerde değişikliğe yol açan çeşitli faktörler vardır. Örneğin her yeni iş fonksiyonu, yeni veya değiştirilmiş bilgi varlıkları ortaya çıkaracak ve her yeni varlık risk değerlendirmesi ve yönetimi sürecinde değişikliklere yol açacaktır.

Risk yönetimi süreci sürekli verimlilik ve etkinliğini geliştirmeyi amaçlayarak devam eden bir faaliyettir. Risk yönetimi süreciyle ilgili; BSI (British Standards Institute), ISO (International Standard Organisation), Proje Yönetim Enstitüsü (Project Management Institute) ve Bilim ve Teknoloji Ulusal Enstitüsü gibi birçok kuruluş çeşitli standartlar geliştirilmiştir.

TS ISO 31000 Risk Yönetimi Standardı kurum veya kuruluşların genel idaresi, stratejisi ve planlaması, yönetimi, rapor verme süreçleri, politikaları, değerleri ve kültürü doğrultusunda risk yönetimi ile ilgili süreci bütünleştirmek amaçlı bir çerçeve geliştirmesine, uygulamasına ve sürekli olarak iyileştirmesine yönelik herhangi karakterdeki riski sistematik, şeffaf ve güvenilir bir şekilde, kapsam ve içerik dâhilinde yönetmek için prensipleri ve genel esasları sağlar.

Bu standart doğrultusunda uygulanacak Risk Yönetimi ile birlikte kurum ve kuruluşların:

- Gelecekte karşılaşılabilecekleri zor durumları öngörebilecekleri,
- Riskler ortaya çıkmadan önlem alınması sağlayabilecekleri,
- Sürpriz ve kayıplarının en aza indirileceği,
- Hızlı ve etkili karar alabilecekleri,
- Zaman tasarrufu sağlayabilecekleri,
- Kaynak israfını önleyebilecekleri,
- Risklerin makul seviyelerde tutulmasını sağlayabilecekleri,
- İs sürekliliği sağlayabilecekleri,
- Hedeflerini gerçekleştirme ihtimalini artırabilecekleri,
- Proaktif yönetiminin teşvik edileceği,
- Risklerin belirlenme ve ele alma ihtiyacı hakkında farkındalık sağlayabilecekleri,
- Fırsat ve tehditlerini analizin edebilecekleri,

- İlgili yasal ve mevzuat şartlarına ve uluslararası normlara uyum sağlama konusunda fayda sağlayabilecekleri,
- Paydaş güvenini ve itimadını iyileştirme konusunda fayda sağlayabilecekleri,
- Karar verme ve planlama için güvenilir bir temel oluşturabilecekleri,
- Riskin ele alınması için kaynakları etkin bir şekilde tahsis etme ve kullanma kolaylığı sağlayabilecekleri,
- Operasyonel etkinliği sağlayıp ve verimliliği artırabilecekleri,
- Kaybın önlenmesi ve vaka yönetimini iyileştirebilecekleri,

belirtilmektedir.

4.1. Bulut Bilişim Risk İşleme

Önceki bölümde bulut bilişim hizmet modelini oluşturan varlıklar ile ilgili tehdit ve zafiyetlerin oluşturduğu riskler belirlenmiş ve belirlenen bu risklerin gerçekleşme olasılıkları ve gerçekleşmeleri durumunda kuruma yükleyeceği maliyetler (etkileri) değerlendirilerek, risk değerleri hesaplanmıştı. Risk yönetiminin ikinci aşaması belirlenen bu risklerin işleme aşamasıdır. Bu aşama risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur. Risklerin tamamen ortadan kaldırılması için bütün kontrollerin uygulanması çoğu zaman mali açıdan imkânsızdır. Bunun için birtakım risk işleme yöntemleri kullanılır. Kuruluş, riski azaltmak istediğinde sisteme gelebilecek zararı en aza indirmek için “en düşük maliyetli” ve “en uygun” kontrolü seçmekle sorumludur. Risk işleme yöntemleri kurumun iş hedeflerine ve misyonuna uygun olarak seçilmelidir. Riski işlemek ve mümkünse kuruluş açısından uygun bir seviyeye indirgemek için kullanılabilecek yöntemler şu şekilde sıralanabilir:

Riskin Kabulü: Potansiyel riski kabul etmek ve BT işletim sistemi sürdürmek veya riski kabul edilebilir bir seviyeye azaltmak için ilgili kontrolleri uygulamak,

Riskten Kaçınma: Riskin nedenini ve/veya sonucunu ortadan kaldırarak riskten kaçınılması (sistemin belirli fonksiyonlarından vazgeçilmesi veya riskler tespit edildiğinde sistemi kapatılması),

Riskin Azaltılması: Bir zafiyet veya tehdidin olumsuz etkisini en aza indirmek gerekli kontrolleri uygulayarak riskini azaltılması (örneğin destekleyici, koruyucu ve belirleyici kontrollerin kullanımı),

Riskin Transferi: Risk etkisiyle oluşabilecek kayıpları telafi etmek için diğer seçenekleri kullanarak riskini transfer etmektir (örneğin sigorta yaptırmak) (Stoneburner, 2002).

Aşağıdaki bölümlerde bu risk işleme yöntemleri kullanılarak bulut bilişim mimarisi için saptanan ve derecelendirilen riskler sırasıyla irdelenecektir. Bulut bilişim mimarisindeki risklerin çok büyük bir bölümü bilgi güvenliği ile ilgili risklerdir. Bu risklerin yukarıda belirtilen risk işleme yöntemleriyle işlenebilmesi için; kurumun kabul edebileceği değerlere düşürülerek azaltılmasını veya tamamen ortadan kaldırılmasını sağlayacak kontrol yöntemleri belirlenmelidir.

4.1.1. Uygun Kontrollerin Belirlenmesi

Zafiyet ve tehditlerin gerçekleşmesini önlemek veya gerçekleşmeleri halinde farkında olmak ve olası etkilerini izleyebilmek için uygulanabilecek kontroller teknik, yönetimsel ve operasyonel kontroller olmak üzere üçe ayrılabilir. Kuruluşlar riskileri azaltmak için önerilen kontrollerin uygulanmasında; teknik, yönetimsel ve operasyonel güvenlik kontrollerini veya bu tür kontrollerin kombinasyonlarını; etkinliklerini maksimize etmek için bir arada düşünmelidir. Her kurum kendine uygun olan kontrol veya kontrolleri maliyet, iş taahhütleri, personel yapısı vb. özelliklerini dikkate alarak belirlemelidir.

4.1.1.1. Teknik Güvenlik Kontrolleri

Teknik güvenlik kontrolleri yazılım, donanım, sistem mimarisi vb. gibi çözümleri içerir. Teknik güvenlik kontrolleri destekleyici, önleyici, tespit edici ve düzeltici olmak üzere dört çeşittir.

Destekleyici Teknik Kontroller: Destekleyici kontroller diğer kontrollerin uygulanmasını sağlayan temel kontrollerdir. Bu kontroller şu şekilde tanımlanabilir.

- **Kimlik tanımlama**: Bu kontrol bir kullanıcının, sürecin veya sistemin eşsiz/benzersiz olarak tanımlanmasında kullanılır. Diğer kontrollerin uygulanabilmesi için (örneğin erişim kontrol listeleri) kimlik tanımlaması şarttır.
- **Kriptografik anahtar yönetimi**: Diğer kontrollerde kriptografik işlemlerin güvenli bir şekilde gerçekleştirilebilmesi için kriptografik anahtar yönetiminin güvenli bir şekilde gerçekleştirilmesi gerekir. Anahtar üretimi, saklanması, dağıtımı ve bakımı kriptografik anahtar yönetiminin içerisindedir.
- **Güvenlik yönetimi**: Bir BT sisteminin güvenlik özellikleri kurumun ihtiyaçlarını karşılayacak şekilde ayarlanabilmelidir. Örneğin bir veritabanındaki bilgileri kimin okuyacağı, kimin oluşturucağı ve kimin güncelleyebileceği ayarlanabilmelidir. Böylece gereğinden fazla yetki verilmemiş olur.
- **Sistem koruma kontrolleri**: Bu kontroller bir sistemin güvenliğinin sağlanabilmesi için gerekli temel konuları içerir. Örneğin bilmesi gereken prensibi, süreçlerin ayrımı, objelerin tekrar kullanılması, katmanlı yapılarda çalışma, güvenilecek nesne sayısının en aza indirgenmesi gibi prensipler bu tip kontrollerdir.

Önleyici Teknik Kontroller: Bu kontroller güvenlik ihlallerinin gerçekleşmesini önleyici kontrollerdir.

- **Kimlik doğrulama:** Bu kontrol kullanıcının belirttiği kimlik tanımlamasını doğrulamaya yarar. Bunun için şifre, PIN numarası, akıllı kart gibi mekanizmalar kullanılmaktadır.
- **Yetkilendirme:** Yetkilendirme bir sistemde izin verilen işlemlerin belirlenmesini ve yönetimin alt birimlere dağıtılabilmesini sağlayan kontroldür.

- **Erişim kontrolü:** Verinin gizliliği ve bütünlüğü erişim kontrolleri ile sağlanır. Bir kaynağa erişim için yetkilendirme yapıldıktan sonra uygun politikalara göre erişim kontrolü sağlanmalıdır. Gizlilik derecesi etiketleri, dosya izinleri, kullanıcı profilleri erişim kontrolünde kullanılan mekanizmalardan bazılarıdır.
- **İnkâr edememe:** Bilgiyi gönderenin gönderdiğini, alanın da aldığını inkâr edememesi sistemin izlenebilirliği açısından önemlidir.
- **Güvenli iletişim:** Günümüzde sık kullanılan dağıtık yapılarda güvenliğin korunmasındaki en önemli faktörlerden biri iletişim sırasında verinin gizliliğinin ve bütünlüğünün korunabilmesidir. Bunun için iletişim sırasında çeşitli şifreleme metotları ve kriptografik önlemler kullanılarak hat dinlemesi, paket dinleme, tekrar gönderme gibi saldırılara karşı önlem alınabilir.
- **İşlem gizliliği (Transaction privacy):** Kişisel işlemlerin gizliliği gittikçe önem kazanmaktadır. Secure Socket Layer (SSL) ve Secure Shell(SSH) gibi teknolojiler kişilerin yaptığı işlemlerin gizliliğinin kaybolmasını engellemek aracıyla kullanılır.

Tespit Edici Teknik Kontroller: Tespit edici kontroller güvenlik ihlalleri gerçekleştikten sonra nelerin, kimin tarafından, ne zaman ve nasıl yapıldığını bulmak için kullanılır.

- **Denetleme:** Güvenlikle ilgili olayların ve sistemdeki anormalliklerin izlenmesi, güvenlik ihlallerinin tespitinde ve olası bir ihlalden geri dönmede en önemli kontroldür.
- **Saldırı tespiti:** Ağ sızmaları ve şüpheli olaylar gibi güvenlik ihlali olabilecek durumların tespiti, uygun kontrolün alınması ve gerekli düzeltmelerin yapılabilmesi için çok önemlidir.
- **Bütünlük:** Sistemin veya verinin bütünlüğünün takip edilmesi, ihlallerin tespit edilmesi açısından önemlidir. Örneğin işletim sisteminin kullandığı dosyalar sadece gerekli işlemler için okunurlar ve bu dosyaların üzerinde değişiklik yapılmaz. Bu dosyaların bütünlüğü virüs veya zararlı bir yazılım tarafından değiştirilirse anti virüs programları bunu tespit edebilir.

Düzeltici Teknik Kontroller: Güvenlik ihlalleri tespit edildikten sonra sistemi eski haline getirmek için kullanılan kontroller bu kategoride incelenebilir.

- **Yedekleme:** Kaybedilen veya bütünlüğü bozulan veri yedeklerden geri dönülerek eski haline getirilebilir.

4.1.1.2. Yönetimsel Kontroller

Yönetimsel kontroller kurumda uygulanan politika, prosedür, standart gibi kuralların uygulanmasını sağlayacak kontrollerden oluşur ve önleyici, tespit edici ve düzeltici olmak üzere üç kategoriye ayrılır.

Önleyici Yönetimsel Kontroller: Önleyici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- BT sistemlerinde güvenliği sağlamak üzere kişilere sorumluluklarının atanması,
- Mevcut ve planlanan kontrollerin dokümante edilmesini sağlayacak sistem güvenlik planlarının geliştirilmesi ve uygulanması,
- Görevlerin ayrılığı, gerekli en düşük yetkilerin verilmesi, hakların tahsis edilmesi ve sonlandırılması gibi personelle ilgili güvenlik kontrollerinin uygulanması,
- Güvenlik farkındalığı ve teknik eğitimlerinin verilerek sistem kullanıcı ve yöneticilerinin bilgi seviyelerinin artırılması,
- Güvenlik politikalarında belirtilen kuralların çalışanlar tarafından bilinmesinin sağlanması,
- Çalışanların özgeçmişlerinin doğrulanması, geçmişlerinin incelenmesi,

Tespit Edici Yönetimsel Kontroller: Tespit edici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- Güvenlik önlemlerinin periyodik olarak test edilmesi,
- Risk yönetiminin uygulanması ve risk işleme için gerekenlerin yapılması,
- Periyodik olarak sistemlerin denetlenmesi,

Düzeltici Yönetimsel Kontroller: Düzeltici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- Sistemlerinin devamlılığının sağlanması ve acil durumlarda veya felaket anlarında BT sisteminin tekrar kullanılabilir hale getirilmesini sağlayacak planların, prosedürlerin ve testlerin yapılmasının sağlanması,
- Acil durum müdahale ekiplerinin kurulması ve yetkin hale getirilmesinin sağlanması,

4.1.1.3. Operasyonel Kontroller

Kurumun güvenlik politikalarının BT varlıklarının kullanılması sırasında doğru şekilde uygulanmasını sağlamak için operasyonel kontrollerin geliştirilmesi ve yönetim tarafından takip edilmesi gerekir. Operasyonel kontroller kurumdaki işlerin yapılması sırasında kasten veya bilmeden yapılabilecek hataları engeller. Bunun için operasyonel kontrollerin nasıl uygulanacağının adım adım açıklandığı dokümanların bulunması ve bu dokümanların kontrolleri uygulayanlar tarafından biliniyor olması gerekmektedir. Önleyici ve tespit edici operasyonel kontroller için bazı örnekler aşağıda verilmiştir.

Önleyici Operasyonel Kontroller:

- Veri ortamlarına erişimin ve veri ortamlarının yok edilmesinin kontrol edilmesi (fiziksel erişim kontrolü uygulanması, veri saklama cihazlarının uygun şekilde imha edilmesi),
- Verinin yetkisiz kişilerin eline geçmesinin engellenmesi (veri sınıflandırma etiketlerinin kullanılması),
- Zararlı yazılım içerebilecek veri kaynaklarının kontrol edilmeden kullanılmasının engellenmesi,
- Ziyaretçilere refakat edilmesi, kimlik kartı taşınması, anahtarların dağıtımının kontrolü gibi fiziksel güvenliği sağlayıcı operasyonel kontroller,
- Yedeklerin alınmasını ve güvenli bir yerde saklanmasını sağlayacak operasyonel adımları içeren kontroller,
- Mobil bilgi işleme cihazlarının kullanım şartlarının belirlenmesi ve güvenliğinin sağlanması,
- Varlıkların yangın, yanlış kullanım vb. sebeplerden etkilenmemesi için uygulanan kontroller (sistem odasında yiyecek ve içecek bulundurulmaması,

yangın tespit ve söndürme sistemlerinin kullanılması, kesintisiz güç kaynakları gibi),

Tespit Edici Operasyonel Kontroller

- Güvenlik kameraları, hareket algılayıcıları ve alarm sistemleri gibi tespit edici fiziksel kontrollerin uygulanması
- Çevresel etkilerin takip edilmesi (duman ve yangın detektörlerinin kullanılması)

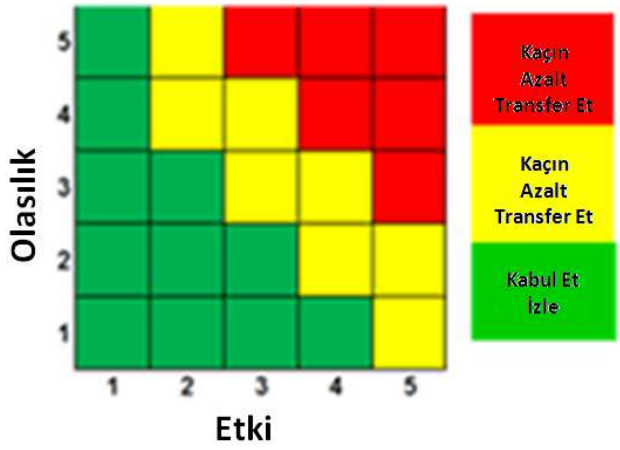
Düzeltici Operasyonel Kontroller

- Yapılan işlerin dokümante edilmesi olası değişikliklerde doğru ayarlamaların tekrar yapılabilmesi,
- Yapılan değişikliklerin dokümante edilmesi ve bir sorun halinde değişiklik yapılmadan önceki duruma geri dönülebilmesi, yapılan değişikliklerden dolayı oluşabilecek sorunların düzeltilmesi, (Eskiyörük, 2007).

4.2. Bulut Bilişim Risklerinin Kabul Edilebilirlikleri

Riskler etkilerinin ve gerçekleşme olasılıklarının bir fonksiyonu olan risk derecelerine göre sıralandıktan sonra risk işleme metodlarına tabi tutulurlar.

Belirlenen risk, daha önceden tespit edilmiş ve tarafımızdan biliniyor, buna karşın gerekli tedbirler alınmış, yeterli gözetim ve kontrol uygulanabiliyor ise risk kabul edilebilir. Hangi risklerin kabul edilebileceği ile ilgili genel kanı; düşük risk değeri olan risklerin kabul edilebilir oldukları yönündedir. Yine Tablo 3.6'da belirtildiği üzere, düşük dereceli risklerle ilgili gerekli kontrol ve önlemlerin uygulanması sistem veya varlık sahibi veya sorumlusunun kararına bırakılmaktadır. Sistem sahibi kuruluş bu risklerin herbiri için belirlenecek kontrol ve önlemleri uygulayabilir veya uygulamaya gerek duymadan riski kabul edebilir. Aşağıdaki tabloda görüleceği üzere yeşil renge boyanmış alanlar içinde kalan düşük risk değerine sahip riskler kabul edilir ve izlenirler. Geriye kalan orta ve yüksek risk değerine sahip riskler ise bir sonraki azaltma, kaçınma ve transfer etme yöntemlerine tabi tutularak işlenecektir.



Tablo 4.1: Risk İşleme Seçenekleri (MITRE Institute, 2010)

Tablo doğrultusunda, önceki bölümde düşük risk derecesi atanan 2,4,17,26,29,32,34 numaralı riskler kabul edilebilir olarak değerlendirilecektir. Aşağıda risk değerlerinin büyüklüğüne göre (büyükten küçüğe) sıralanan bu risklerle ilgili, önceki bölümde bahsedilen teknik, yönetimsel ve operasyonel kontrol ile birlikte risklere özgü önlemlerin başlıcaları aşağıda sıralanmaktadır. Belirtilen bu kontrol ve önlemlerin uygulanması veya uygulanmadan riskin kabulü tamamen sistem/varlık sahibinin kararına bağlıdır.

R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık: Düşük dereceli risklerin en yüksek risk değerine sahip olanlarından biri olan bu risk; bulut sağlayıcıları ile müşteri kuruluşların sorumluluklarının tam olarak farkında olmaları ve yine müşterilerin bulut mimarisi üzerinden gerçekleştirecekleri iş ve işlemlerine ait gereksinim ve isterlerini detaylı bir şekilde belirlemeleri durumunda kabul edilebilir bir nitelik kazanır. Sorumluluk, gereksinim ve isterlerinin bilincinde olan kuruluş, bu doğrultuda hizmet temin edeceği sağlayıcıyı seçecek ve gerekli gördüğü her ayrıntıyı sözleşmeyle kayıt altına alabilecektir. Yine de spesifik olarak aşağıdaki kontrol ve önlemleri uygulaması kuruluşun yararına olacaktır.

Bu riski önlemek için müşteri kuruluş,

- Sağlayıcı tercihi yapmadan önce, muhtemel sağlayıcıların sistemlerini iyi incelemeli, sağlayıcıdan kendi iş gereksinimleri doğrultusunda hizmet satın almalı ve sağlayıcının ilgili hizmetleri sunacağını eksiksiz bir şekilde bağlayıcı bir sözleşmeyle kayıt altına almalıdır.
- Sağlayıcıya yaptıracağı güvenlik ve uyum ile ilgili kontroller hakkında kesin bir kanaate sahip olmalıdır. Çünkü bu kaanat kuruluşun kendi uygulaması gereken özel izleme kontrollerini belirleyecektir.
- Bulut çözümü kontrol ortamının yürütülmesinin, sağlayıcı ile kendisinin ortak sorumluluğu olduğunun bilincinde olup, her iki tarafın sorumluluk sınırlarını sözleşmeyle belirlemelidir.
- Ayrıca kuruluşun kontrol ortamının içine tamamlayıcı kullanıcı varlık kontrolleri dâhil edildiğinden emin olmalıdır.
- Sağlayıcı hizmetlerinde müşterilerinin sorumluluklarını tanımlayan ve böylece bu görevleri sağlayıcı kontrol sorumluluklarından hariç tutarak tamamlayıcı bir kullanıcı varlık denetim bileşeni içeren, üçüncü taraf denetim raporlarının hazırlanmasını sağlayıcıya şart koşmalıdır.
- Sağlayıcının sorumluluklarını alt yüklenicilerine taşere etmek istemesi durumunda, ya tüm geçerli alt yükleniciler için denetim raporlarını hazırlanmasını; aksi takdirde, ilgili kuruluşa sağlanan hiçbir hizmette taşeron kullanmayacağını sözleşmeyle taahhüt etmesini istemelidir.
- Periyodik olarak sağlayıcı tarafından sağlanan kontrollerin etkinliğini doğrulamalıdır.

R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması: İlgili kayıtların yasal olarak belli bir süre tutulması zorunluluğu olmasına rağmen, kuruluşun hizmet ve iç faaliyetlerinde kesinti yaratmayıp çok ciddi sonuçlar doğurmayacağından gerekli önlem ve kontrollerin alınması şartıyla kabul edilebilecek bir risktir. Hem müşteri kuruluş ve hem de sağlayıcı tarafından saklanabilecek olan bu kayıtların bozulması veya kaybolması riskini önlemek için, müşteri kuruluş ve sağlayıcılar tarafından aşağıdaki önlem ve kontroller uygulanabilir:

- Güvenlik cihazlarına, veri tabanlarına ve network cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
- Sunucularına ve servislerine sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.
- Merkezi kayıt sunucuları üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalı ve uyarı olarak yetkili birimlere gönderilmelidir.
- Merkezi kayıt sunucuları üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.
- Merkezi kayıt sunucuları üzerindeki kayıt verileri belirli tarih aralığında tutulmalı, istenildiğinde raporlanabilmeli ve yapılacak analizler doğrultusunda saldırı ve normal olmayan durumları tespit edilip uyarılar gönderilebilmelidir (Öztürk, 2014).
- Sistemlerinde yeniden yapılandırma dönemlerinde kayıtların kaybolması önlenmelidir.
- Log kayıtlarının ne kadar süreyle tutulmasının zorunlu olduğuyla ilgili adli mevzuat sürekli olarak takip edilmeli ve bu yönde gerekli aksiyonlar alınmalıdır.

R.29- Hizmet Ücreti Değişikliği: Birim hizmet maliyeti değişimi riski, ücretlendirme politikasının sözleşmeyle kayıt altına alınması durumunda kayıt altına alınması durumunda kabul edilebilecektir. Yine de bu riski azaltmak için kuruluş:

- Hizmet maliyetlerinin ve maliyet değişikliklerinin hizmet sözleşmesinde tanımlanmasını sağlamalıdır.
- Her sözleşme yenileme sırasında, hizmet ilişkisinin maliyet, fayda, risk, değiş dokuş dengesini hesaplamalıdır (Mosher, 2011).
- Bilişim kaynağı miktarı veya kullanım zamanı birim fiyatına göre ücretlendirilen hizmetlerde temin ettiği kaynağın belli kullanım limitlerinin üstüne çıkması durumunda; ilgili birim fiyatlarda indirim talep etmeli ve bu durumu sözleşmeyle kayıt altına almalıdır.

R.2- Bulut Hizmeti Sonlandırması veya Arızası: Bulut sağlayıcı kuruluşların iflası, devri, hizmet kapsamını değiştirmesi veya hizmetlerini taahhüt ettiği şekilde yerine getirememesi, diğer bütün hizmet sektörlerinde olduğu gibi bulut bilişim sektöründe de görülebilecek risklerdir. Bu tip durumlar sebebiyle sağlayıcının hizmetlerinde meydana gelebilecek sonlandırma veya arızalar; müşteri kuruluşun alacağı birkaç önlemin ardından kabul edilebilir. Bu doğrultuda riski önlemek için kuruluşlar:

- Kendi sağlayıcılarıyla aynı veya benzer mimariler ve yazılımlar kullanan diğer sağlayıcılarla anlaşarak; verilerinin kopyalarını koruyabilirler, böylece herhangi bir hizmet sonlandırması durumunda sistem kolayca yedek sağlayıcıya aktarılabilir.
- Arızalara karşı sistem kullanılabilirliğini izlemek için gerekli süreçleri uygulayabilirler.
- Başka bir servis sağlayıcıdan bulut hizmetleri için, talep üzerine kaynak aktarımı sağlayan otomatik araçları ihtiyaç anında devreye alabilirler.
- Hizmet seviye anlaşmalarına, sağlayıcı kaynaklı sistem arızaları durumunda; hızlı ve yeterli müdahalenin sağlanacağına ilişkin bağlayıcı ve cezai şartlar içeren maddeler ekleyebilirler.
- Olası bir hizmet sonlandırması durumunda tüm veri ve uygulamalarının eksiksiz şekilde teslim edileceğine dair şartları hizmet seviye anlaşmasına ekleyebilirler.

R.4- Üçüncü Parti Tedarikçi Hatası: Sağlayıcının hizmetlerinin bir kısmını taşere ettiği alt yükleniciler genel olarak sağlayıcı kuruluşa oranla daha küçük boyutta işletmeler olup, hizmetlerin güvenliği, gizliliği ve kullanılabilirliği ile ilgili sağlayıcılar kadar bütçe ayıramazlar ve bu da müşteri açısından riskler yaratabilir. Yine de müşteri kuruluşların, bu tip alt yüklenicilerin eksikleri veya hatalarıyla ilgili sağlayıcılarla yapacakları sözleşmeye ekleyecekleri birkaç madde hem kendilerini ve hem de sağlayıcıyı olası risklere karşı güvenceye alıp, riskin kabul edilebilirliğini pekiştirebilir. Bu amaçla kuruluş aşağıdaki önlemleri alabilir:

- Düzenleyici ve yasal gereksinimleri karşılamak için bir yükümlülük altındaysa, bulut hizmeti sağlayıcısından alt yüklenicilerinin uyum durumlarını kontrol etmek için kimliklerini sağlamasını talep etmelidir.
- Eğer uyum izleme bu düzeyde gerekli değilse; servis sağlayıcıdan, tüm şartlara uymaya zorlaması için bu sağlayıcılarla sözleşme yapmasını talep edebilir.
- Servis sağlayıcısından, satıcılarının şartlara uyumu izlemek için bir satıcı yönetim programı uygulamasını talep edebilir ve bu sayede servis sağlayıcının alt yüklenicilerinin uyumunu izleyebilir (Mosher, 2011).
- Olası alt yüklenici değişimlerinde, yeni alt yüklenicinin uygunluk durumunun bildirimi ile ilgili sözleşmeye gerekli şartları ekleyebilir.

R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması: Günümüzde fiziksel güvenlikle ilgili yaşanan gelişmeler ve birbiri ardına ortaya konan yeni teknolojiler, veri merkezlerinin güvenlikle ilgili risklerini hem sağlayıcı ve hem de müşteri kuruluşun kabul edebileceği seviyeye indirgemiştir. Yine de bu riski önlemek için müşteri kuruluş sağlayıcının,

- Bilgi işleme servisini korumak amacıyla fiziksel sınır güvenliği tesisi kurulmuş olmasını (Kart kontrollü giriş, duvarlar, güvenlik personeli bulunan nizamiye) şart koşmalıdır.
- Fiziksel sınır güvenliğini, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalarını talep etmelidir.
- Veri merkezleri içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurmasını ve hassas bilgilerin bulunduğu alanları kimlik doğrulama ve pin koruması gibi yöntemlerle yetkisiz erişime kapatılmasını talep etmelidir.
- Yedeklenmiş materyal ve yedek sistemlerini ana tesisten yeterince uzak bir yerde konuşlandırmış olduğunu teyit etmelidir.

- Güvenli alanlarına kayıt cihazlarının sokulmasına engel olmasını, kötü niyetli girişimlere engel olmak için bu bölgelerde yapılan çalışmalara nezaret edilmesini ve yapılan girişlerin kayıt altına alınmasını talep etmelidir.
- Bilgi işlem servisleri, dağıtım ve yükleme alanlarıyla, yetkisiz kişilerin tesislere girebileceği noktaların birbirinden izole edilmiş teyit etmelidir.
- Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PCler vb. cihazlarını yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde bırakmadığını onaylamalıdır.
- Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması ile ilgili gerekli önlemleri aldığından emin olmalıdır.
- Ekipmanlarının bakım için kurum dışına çıkarılması durumunda, kontrolden geçirilmesini ve içindeki hassas bilgiler silinmesini talep etmelidir.
- Ekipmanı imha edilmeden önce içinde gizli bilginin bulunan depolama cihazının fiziksel olarak imha edildiğinden veya depolama cihazının içerdiği bilginin bir daha okunamaması üzere geri döndürülemez şekilde silindiğinden emin olmalıdır.
- Ekipmanının, verisinin veya yazılımının yetkilendirme olmadan tesis dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturmasını talep etmelidir (Öztürk, 2014).

R.32- Doğal Afetler: İnsanlığın var oluşundan beri ciddi yıkımlara sebep olan doğal afetler birçok durumda önlenmesi imkânsız olan olaylardır. Ancak doğru kontrollerle etkileri azaltılabilir. Ciddi etkileri olsa da aynı bölgelerde genelde çok nadiren meydana gelmeleri ve önlenmeleri ile ilgili aksiyon almanın zorluğu veya imkânsızlığı nedeniyle kabul edilebilir risk grubuna dâhil edilmektedirler. Müşteri kuruluşlar doğal afetlerin bilişim altyapısında oluşturdukları risklere karşı sağlayıcı seçiminde aşağıdaki başlıca kontrolleri göz önünde bulundurmalıdır. Bu doğrultuda kuruluş sağlayıcının:

- Acil durumlar için acil durum ekibi belirlediğini ve eğittiğini teyit etmelidir.

- Acil durum ihbarı gelmesi durumunda tüm dâhili ve harici ilgisiz telefon görüşmelerini keserek süratle ilgili tüm birimlere bilgi vermesini istemelidir.
- Acil durum eylem planları oluşturduğundan ve bu planlarının ihtiyaç olmaksızın test ettiğinden emin olmalıdır.
- Acil durum eylem planı test programından elde ettiği bulguları, prosedürleri, dokümantasyonu sonraki acil durum eğitimlerine dâhil etmesini istemelidir.
- Veri merkezlerini doğal afet riski yüksek bölgelere kurmadığını teyit etmelidir.
- Personelinin acil durumlarda alacağı görevler ile ilgili görsel ve yönlendirici işaretlerin veri merkezlerinde bulunmasını talep etmelidir.

Daha önce belirtildiği üzere burada sıralanan önlem ve kontrollerin her birinin ayrı ayrı uygulanması kararı tamamen sistem/varlık sahibine aittir. Bu önlemler ve kontroller için gerekli zaman, maliyet ve iş yükü müşteriden müşteriye değişebilecek olup, müşterinin iş kapsamının büyüklüğüne ve kritikliğine bağlı olarak ilgili faaliyetlerin gerçekleştirilmesi verimsiz gözükebilir. Ayrıca bu durumun tam tersi şekilde bu çalışmada düşük risk değerine ve derecesine atanan ilgili risklerin bazıları, bazı kuruluşlar için orta hatta yüksek risk derecesi taşıyabilir. Örneğin deprem bölgesi içinde bulunan bir bölgede doğal afet riski orta dereceli risk grubuna dâhil edilebilir. Bu durumda müşteri kuruluşların ilgili kontrol ve önlemleri uygulamaları zorunlu hale gelebilir.

4.3. Bulut Bilişim Risklerinin Değerlerinin Azaltılması, Transferi veya Risklerden Kaçınılması

Tablo 3.6'da belirtildiği üzere, risk işleme yöntemlerinin uygulanması orta risk derecesine sahip riskler için gerekli, yüksek dereceli riskler için ise zorunludur. Bu sebeple bu bölümde, önceki alt başlıkta kabul edilebilir olanları belirtilen risklerin geri kalanları, risk değerlerine göre sıralanıp risk işleme yöntemlerine göre işleneceklerdir. Risklerle ilgili Tablo 3.6'da da belirtildiği gibi, orta ve yüksek dereceli riskler için azaltma, transfer ve kaçınma yöntemlerini uygulamak gerekmektedir. Bu doğrultuda öncelikle risk değerlerinin azaltılmasına yönelik gerekli teknik, yönetimsel ve

operasyonel kontrol ve önlemlere yer verilecek, ardından ilgili risklerin üçüncü taraflara transfer edilmesi ve riskten kaçınmak için ilgili hizmetin tümünün veya belli bir kısmının kullanılmaması yöntemleri irdelenecektir.

Risk yönetiminde risklerin değerlerinin azaltılması; ilgili riskin kapsamı, meydana gelme olasılığı ve etkileri göz önünde bulundurularak; gerekli önlem ve kontrollerin belirlenmesi ve uygulanmasıyla mümkün olacaktır. Kuruluşlar risk kontrol seçeneklerini geliştirirken, diğer müşterilerin benzer riskli durumlardaki potansiyel çözümlerini kendi iş kapsamlarına uyarlarlar. Başka bir kuruluşun ilgili riske yönelik çözümü değerlendirilirken, her iki kuruluşun mimarileri arasındaki farkları ve bu farkların ilgili kontrollere etkilerini değerlendirmek, müşteri kuruluşun faydasına olacaktır.

Risk yönetiminde genel olarak, meydana gelme olasılığı yüksek fakat kuruluşa finansal etkileri düşük risklerin, risk değerlerinin öncelikli olarak azaltılmasına çalışılır. Ancak bu çalışmada orta ve yüksek değere sahip risklerin herbiri için başlıca önlem ve kontrol seçeneklerine yer verilecektir.

Bir diğer risk işleme yöntemi olan risk transferinde kuruluşlar ilgili risk alanı için başka bir kuruluşa hesap, sorumluluk veya yetki atayabilirler. Ancak başka bir kuruluşa risk transferi, iş operasyonları ve prosedürleri ile ilgili bağımlılıklara ve kontrol kaybına neden olabilir. Bu sebeple, transfer seçeneğini uygulamak için kuruluşların kendi özel ihtiyaçlarının ve bu ihtiyaçlara özel çözümlerin farkında olması ve tedarik ettiği hizmeti buna uygun şekilde talep etmesi gerekecektir.

Kamu kuruluşları için bulut bilişimde risk transferi, bazı risklerin sigortalatmak suretiyle sigorta şirketlerine devri gibi genel bir transfer seçeneğinin yanında; bulut hizmetiyle ilgili risklerin bir kısmının kamu bulut sağlayıcısı ajans/kuruma, kamu BİT sağlayıcısına veya bulut aracısına devri şeklinde de uygulanabilir (Bkz: Kamu Bulutu İşletme Modelleri). Burada kamu bulutu sağlayıcısı kurum veya şirket ile bulut aracıları, doğal olarak bulut mimarisindeki zayıflıklar ve tehditler hakkında daha tecrübeli olduklarından, bunların ortaya çıkardığı risklerin azaltılmasıyla ilgili kontrol ve

önlemleri uygulamak ve sözleşmeleri bu doğrultuda düzenlemek konularında müşteri kuruluşun yükünü hafifletebilir ve belli başlı konularda sorumluluğu üstlenebilirler.

Tüm kontrol ve önleme yöntemlerine rağmen hala riskin ciddi etkilerinin olabileceğinin anlaşıldığı durumlarda, ilgili riskten kaçınmak için işin hepsinden veya bir kısmından vazgeçmek doğru yöntem olacaktır.

Genel olarak risk olasılığı düşük fakat etkileri, özellikle de finansal etkileri yüksek risklerin; mümkün olduğunca üçüncü taraf kuruluşlara transfer edilmesi uygun olacaktır. Hem risk olasılığı ve hem de risk etkisi yüksek riskler içinse, riskten kaçınma yöntemlerini uygulamak doğru bir yaklaşımdır.

Aşağıda en yüksek risk değerinden başlayarak azalan risk değerlerine göre, öncelikle risk değerlerini azaltmak için belirlenen başlıca kontrol ve önlemler sıralanmış olup; hemen ardından ilgili riske dair eğer varsa transfer ve kaçınma seçeneklerinden bahsedilecektir.

R.1- Yönetim ve Kontrol Kaybı: Bu risk bulut bilişimle ilgili belirlenen en yüksek risk değerine sahip olan risktir. Kuruluşların, bulut sağlayıcıların altyapısı üzerinde barındırdıkları (IaaS) veya ilgili altyapı üzerinden kullandıkları (PaaS, SaaS) uygulamaları ile verilerinin kontrolünü kaybetmeleri riski; veri kontrol, yönetim ve denetimini belli ölçüde kullanıcıya bırakan sağlayıcıların seçilmesi ve bu durumun sözleşmede kayıt altına alınması yöntemleriyle azaltılabilecektir. Ancak yine de diğer risk işleme yöntemlerini uygulamak gerekebilecektir. Bu riskin azaltılabilmesi için alınabilecek önlem ve kontroller şu şekildedir:

- Hizmet satın almadan önce teklif veya değerlendirme sürecinde, kuruluş bu risk ile ilgili yaşayabileceği problemleri göz önünde bulundurarak, sağlayıcının faaliyetleri ve kontrol süreci hakkında sorular içeren bir dökümanı cevaplamasını talep etmeli ve seçimini bu döküman doğrultusunda şekillendirmelidir.
- Kuruluşlar sağlayıcı ile yapacakları sözleşmelere, denetim hakkı maddeleri eklemeye çalışmalıdır.

- Sağlayıcının iç kontrol ortamı değerlendirilmesi kapsamında, kuruluş sağlayıcıların belirli risk olaylarını ne şekilde ele aldığını ve ne şekilde yönettiğini belirlemelidir.
- Kuruluşlar, sağlayıcının iç kontrol ortamının bulut çözümü ve kalitesi hakkında daha fazla bilgi için, kendi iç denetim fonksiyonu oluşturmalı ve sağlayıcıdan güvenlik, kullanılabilirlik, işlem bütünlüğü, gizlilik veya veri mahremiyeti konularında raporlar içeren, bağımsız denetim raporlarını ilgili denetim firmalarına hazırlatmalarını talep etmelidir.
- Sağlayıcının veri sınıflandırma politikaları, hassas sayılabilecek bilgi türlerini, kuruluşun doğrudan kontrolü dışında barındırılmaması gereken verileri ve bu bilgilere ve verilere erişme yetkisi bulunacak sahiplerini açıkça tanımlamalıdır (Horwath, 2012).
- Hizmet seviye anlaşmalarında, kuruluşların veri güvenliği amacına yönelik ihtiyaç duyabileceği; port taramaları, güvenlik açığı değerlendirmeleri ve penetrasyon testleri gibi faaliyetlerinin kapsamını tanımlayan şartlara yer verilmelidir.

Riskin transferi: Yönetim ve kontrol kaybı riskinin başka bir kuruluşa (kuruma, kamu BİT sağlayıcısına veya bulut aracısına) transferi, müşteri kuruluşun bu defa verinin kontrol ve yönetimini bu kuruluşa devretmesine yol açacağından çok anlamlı değildir. Fakat yine de, bu riskle ilgili teknik anlamda yeterli bilgi ve tecrübesi bulunmayan kuruluşların, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına bu konuda gereksinimlerini bildirerek; bu riski minimize edecek hizmet seviye anlaşmalarını ilgili sağlayıcılarla imzalamalarını temin edebilir.

Riskten Kaçınılması: Müşteri kuruluşlar, kritik veriler içeren, güvenlik ve gizlilik politikalarının kendilerinin denetiminde olması gereken hassas uygulamalarını; ilgili kuruluş denetimi ve bağımsız denetim imkânı sunmayan ve ayrıca sözleşmelerinde bu şartlara yer vermeyen sağlayıcılarla sözleşme imzalamayarak bu riskten kaçınabilirler.

R.6- Uyum Sorunları: Hizmetlerini çağımızın bilişim trendi olan bulut bilişim mimarisi üzerinden sunmayı hedefleyen kuruluşların bir bölümü özellikle veri mahremiyeti,

güvenliği ve kullanılabilirliği ile ilgili teknik veya yasal uyum sorunları yaşayabilmektedirler. Bu sorunu aşmak için müşteri kuruluşun sunacağı hizmetlerin yasal ve teknik gereksinimlerini iyi bilmesi ve sözleşme imzalayacağı sağlayıcının bu gereksinimlere cevap verebileceğinden emin olması gerekmektedir. Yine sağlayıcının ilgili standartlara uyumu ile ilgili zaman içinde ortaya çıkabilecek aksaklıklara karşı denetim mekanizması oluşturulması, kuruluş açısından önem arz etmektedir. Uyum riskini azaltmak için;

- Kuruluş yürüteceği iş ile ilgili zorunlu standartları belirlemeli ve bu standartlara servis sağlayıcısının uyumunu doğrulayan bir uygunluk doğrulama programı uygulamalıdır.
- Kuruluş sözleşmede belirtilmek şartıyla, ya kendi denetim ekibi tarafından gerçekleştirilen bir denetim yoluyla veya üçüncü bir taraf doğrulaması aracılığıyla; SOC 1, SSAE 16, SOC 3 formatındaki raporları kullanarak, servis sağlayıcının destek sistemlerinin denetlenebileceği ve doğrulanabileceği bir mekanizma oluşturulmasını talep edebilir.
- Kuruluş eğer varsa bir önceki servis sağlayıcının hazırladığı SAS 70, SSAE 16 formatındaki raporların kopyalarını kullanarak, sağlayıcı ile ilgili düzenli denetimler yürütebilir (Mosher, 2011).
- Kuruluşlar yine hizmet altyapısı sunan telekomünikasyon sağlayıcısı değişikliği durumunda, hizmet aldıkları sağlayıcının bu değişimlere ne şekilde ayak uydurabileceğini bilmesi ve bu esnekliği talep etmesi gerekir.

Riskin transferi: Yürüteceği işlerle ilgili gereksinim duyacağı standartları belirleyemeyen veya bu standartlarla ilgili denetimleri belirleyip, yönetemeyen kuruluşlar; bu işlerin sorumluluğunu gerekli sözleşmelerle bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına aktarabilirler.

Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar, bulut kaynaklarını yasal uyumluluk gereksinimleri olmayan veri uygulamaları için kullanabilirler.

R.20- Yargı Değişiminden Kaynaklanan Riskler: Kuruluşların veri ve uygulamalarının farklı yargı mevzuatı bulunan ülke veya bölgelerde barındırılmasının yaratacağı riskleri bertaraf etmek için, öncelikle kuruluşlar bulut altyapısındaki verileri ile ilgili bağlı olduğu mevzuatın ne gibi yasal yükümlükler içerdiğini iyi bilmelidir. Ancak bu şekilde veri gizliliği ve güvenliği gibi konulardaki yasal gereksinimlerini sağlayıcı firmadan talep edebilir. Yine kuruluşun, sağlayıcının verilerini hangi lokasyonlarda saklayacağı konusunda bilgisi ve hukuksal bir dayanağının bulunması şarttır. Bu doğrultuda riski azaltmak için müşteri kuruluş:

- Yasal ve düzenleyici gereklilikleri değerlendirmeye alarak, verilerinin belirli bir yasal yetki alanı dışında saklanabilmesi ile ilgili bir kısıtlamanın olup olmadığını belirlemelidir. Eğer bu tür bir kısıtlama ile karşı karşıya kalırsa, hizmet sağlayıcısı ile bu konuyu müzakere etmelidir.
- Sözleşmeye depolama konumunun kısıtlanmasıyla ilgili, kendi yasal ihtiyaçları ile uyumlu maddeler koymalıdır.
- Verilerinin lokasyonuyla ilgili sözleşme şartlarının tespiti aşamasında, sağlayıcının bulunduğu ve verilerinin muhtemelen depolanabileceği ülkelerin veri koruma kanunlarını uyum açısından değerlendirilmelidir.
- Sağlayıcıdan, farklı bir ülkede verisini barındırması durumunda, bu durumun kendisi için doğuracağı yasal sonuçlar; yabancı bir mahkemenin kendisinin veya müşterilerinin verileri ile ilgili celp göndermesi halinde yasal hakları, aynı fiziksel kaynağı paylaştığı farklı bir müşteri ile ilgili mahkeme celbi durumunda, farklı müşterilerin verilerini birbirinden ayıracak izolasyon yöntemleri olup olmadığı konularında bilgi talep etmelidir.
- İlgili ülkenin kolluk kuvvetleri veya sivil görevliler tarafından mahkeme celbi sonucu sağlayıcının fiziksel donanımına el konulması durumunda, verilerini farklı yasal çerçeveye sahip ülkelerde barındırmasının, kendi kullanıcılarının yasal haklarını ihlal edip etmeyeceğini irdelemelidir.

Riskin transferi: Yürüteceği işlerle ilgili gereksinim duyacağı standartları belirleyemeyen veya bu standartlarla ilgili denetimleri belirleyip, yönetemeyen

kuruluşlar; bu işlerin sorumluluğunu gerekli sözleşmelerle bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına aktarabilirler. Ayrıca, sağlayıcılarının muhtemel veri saklama lokasyonlarının yasal mevzuatı ile kendi tabi oldukları yasal mevzuatın karşılaştırılması ve bu yolla verilerinin barındırılmasının risk yaratmayacağı ülkeleri belirlemek amacıyla, uluslararası hukuk bürolarıyla çalışabilirler.

Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar, veri ve uygulamalarını farklı yargı mevzuatı bulunan bölgelerde barındıran sağlayıcılarla çalışmamalıdırlar.

R.13- Şifreleme: Bulut mimarisinde verilerin şifrelenmesiyle ilgili risklerin önüne geçilebilmesi için temel gereksinimler, kuruluşların verilerinin hassasiyet seviyelerinin ve bu hassasiyet seviyelerini karşılayacak şifreleme yönteminin farkında olmalarıdır. Bu hususların farkında olan kuruluş aşağıdaki kontrol ve önlemleri uygulayarak riski azaltabilir.

- İhtiyaç duyulan düzeyde şifreleme sağlayan bir bulut servis sağlayıcı seçebilir.
- Servis sağlayıcının uygun şifreleme kontrolleri uyguladığından emin olmalıdır.
- Servis sağlayıcının şifreleme kontrollerini düzenli olarak test ettiğinden emin olmalıdır.
- Şifrelemeyi desteklemek için uygun şifre anahtar yönetim uygulamalarının kullanıldığından olduğundan emin olmalıdır.
- Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için, sayısal imzaların veya mesaj doğrulama kodlarının kullanıldığından emin olmalıdır.
- Kripto kullanımı ile hangi iş bilgisinin korunacağı ile ilgili genel prensipler belirlemelidir.
- Sunuculara kriptolu bağlantı ile bağlanılmasını ve düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portların kapatılmasını talep edebilir.
- Risk belirleme esasına dayalı olarak gereksinim duyulan koruma seviyesi ile şifreleme algoritmasının türü, gücü ve niteliğini ortaya koymalıdır.

- Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımını belirlemelidir (Öztürk, 2014).
- Şifrelenmiş bilgi kullanımının kuruluşun sunduğu hizmetlerde veri aktarım hızına ve dolayısıyla hizmetlerin kullanılabilirliğine etkilerini değerlendirmelidir.

Riskin transferi: Müşteri kuruluş verilerinin hassasiyet seviyelerinin ve bu hassasiyet seviyelerini karşılayacak şifreleme yönteminin tespiti ve şifre anahtarlarının yönetimi görevleri, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devredilerek şifreleme riski belli ölçüde transfer edilebilir ancak özellikle hassas veriler içeren uygulamaları yöneten kuruluşların şifreleme yönetimini bizzat uygulaması gerekmektedir.
Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar bulut servislerini, veri gizliliği amacıyla şifrelemesi gereken veriler için tercihen kullanmayabilirler.

R.24- Veri Koruma Riskleri: Veri koruma, kuruluşların verilerinin güvenliği ve gizliliğinin ne ölçüde korunduğuyla ilgili, sağlayıcılardan aldıkları geri bildirimlerle ve bu konuda yaptıkları denetimlerle doğru orantılıdır. Kuruluşların veri koruma hususunda sağlayıcılarla işbirliği içinde olması ve güvenlik ihlallerine karşı ortak tedbirler alması gerekmektedir. Bu amaçla veri koruma riskini azaltmak için müşteri kuruluş:

- Olası bir ihlal durumunda her seferinde müşterisine haber vereceğini sözleşmede taahhüt eden bir bulut servis sağlayıcısı ile sözleşme yapabilir.
- Sağlayıcıdan bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan, uygun bir geri besleme süreci oluşturmasını talep etmelidir.
- Sağlayıcıdan, bilgi güvenliği ihlâli oluşması durumunda, ilgili kişilerin tüm gerekli faaliyetleri yürütmesini sağlamak maksadıyla; bilgi güvenliği olayı rapor formatı hazırlanmasını ve güvenlik olayı oluşması durumunda anında raporlamasını talep etmelidir.
- Sağlayıcıdan, güvenlik ihlaline sebep olan kullanıcının müşterileri veya çalışanları olması durumunda; gerekli önlemleri alması, yaptırımlarda bulunması ve ihlal raporunu en kısa sürede kendisine sunmasını talep edebilir.

- Sağlayıcının bilgi sistemi arızaları, hizmet kayıpları, zararlı kodlar, DOS atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler almış olduğunu, hizmeti kullanmaya başlamadan önce teyit edebilir.
- Sağlayıcının normal olasılık planlarına ilave olarak, olayın tanımı ve sebebinin analizi, tekrarını önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konularında çalışmalar yapmasını talep edebilir.
- Sağlayıcıdan, sunduğu hizmetlerle ilgili bir Bilgi Güvenliği Sistemi oluşturup düzenli bir şekilde denetlemesini, bütün birimleri kapsayacak şekilde iç denetim planı hazırlanmasını, ilgili denetimlerin sonuçlarının iç denetim raporu şeklinde hazırlanarak kendisine sunulmasını ve tespit edilen bulgular için çözüm önerileri geliştirilerek, bu bulguların çözümlenip çözümlenmediği hususunun takip edilmesini isteyebilir.

Riskin transferi: Müşteri kuruluş, veri işleme sertifikasyon kontrolleri, farklı ülkelerdeki veri koruma yasalarının takibi, bilgi güvenliği ihlallerinin bildirilmesi ve bu doğrultuda gerekli aksiyonların alınması gibi sağlayıcı sorumluluklarının takibini, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devrederek, riskin bir kısmını transfer edebilir.

Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar, bulut servislerini sadece yasal uyumluluk gereksinimleri olmayan veri uygulamaları için kullanabilir.

R.14- Kaynak İzolasyonu Eksikliği: Sanallaştırma teknolojileri yardımıyla, aynı fiziksel donanım üzerinde birden çok müşteriye hizmet vermek için geliştirilmiş bulut mimarilerinde, bazı kullanıcıların diğer kullanıcıların verilerine sızması veya saldırmasını önlemek için sanal kaynaklar içerisinde bölümlendirme ve yetkisiz erişim engellemeleri son derece önemli hale gelmektedir. Bu sebeple müşteri kuruluş verilerinin hassasiyeti ölçüsünde, sağlayıcının kaynaklarında gerekli izolasyonun

sağlanmasını ve bu işlemin etkinliğinin sürekli olarak izlenmesini talep etmelidir. Bu doğrultuda aşağıdaki kontrol ve önlemler ilgili riskin azaltılmasına yönelik kullanılabilecektir.

- Sağlayıcı, farklı kuruluşların veri ve uygulamaları arasında, ilgili verilerin hassasiyeti ölçüsünde iç engeller ve bölümlemeler (segmentasyon) uygulayabilir.
- Müşteri kuruluş, engellerin ve bölümlendirmelerin etkili olduğunu doğrulamak için veri depolama denetimleri yürütmeyi talep edebilir.
- Müşteri kuruluş, kaynak izolasyon eksikliği sebebiyle yaşanabilecek konuk atlamalı saldırılar, SQL enjeksiyon saldırıları, yan kanal saldırıları vb. durumların sağlayıcı tarafından izlenmesini ve bu saldırılarda bulunan müşterilere gerekli yaptırımların uygulanmasını talep edebilir.
- Kuruluş hizmet seviye anlaşmasıyla, satıcının izolasyon eksikliği kaynaklı risklerle ilgili belirlenmiş şartlara uyumunu zorunlu kılabilir ve izleyebilir.

Riskin transferi: Müşteri kuruluş, kaynak izolasyon uygunluk denetimlerini bağımsız denetim firmalarına, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devrederek, riski transfer edebilir.
Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar, iç bölümlendirme ve kaynak izolasyonu seçenekleri sunmayan sağlayıcıların kaynaklarını kullanmayabilirler.

R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş: Kuruluşların, verilerine kötü niyetli erişim sağlayarak görevini istismar edebilecek, verilerini maddi veya diğer yaşadışı amaçları için kullanabilecek sağlayıcı personeline karşı, sağlayıcılardan tam güvence alma zorunlulukları bulunmaktadır. İlgili personelin zararlı faaliyetlerinin önlenmesi ve riskin azaltılması için müşteri kuruluş sağlayıcıdan:

- Personelini ve özellikle de sistem yöneticisi ve denetçilerini, detaylı bir şekilde güvenlik soruşturmasına tabi tutmasını ve sicilinde suç unsuru bulunan kişileri yetkilendirmemesini talep etmelidir.

- Bütün personelini iç denetime tabi tutmasını, kötü niyetli veya kusurlu işlem gerçekleştiren kullanıcılarının kritik verilere erişim yetkisini kısıtlamasını talep etmelidir.
- Yüksek ayrıcalıklı rollere sınırlı sayıda ve uzun süre yasal bir şekilde hizmet etmiş personelin görevlendirilmesi konusunda teyit almalıdır.
- Personelini suç çetelerinin hedefi olmaktan korumak için gerekli güvenlik tedbirlerini almasını ve bu konuda pesonelinde farkındalık yaratmasını istemelidir.
- Özellikle yüksek ayrıcalıklı rollere atadığı personelin güvenlik ve operasyonel log kayıtlarını periyodik olarak incelemesini talep edebilir.

Riskin transferi: Bu risk de tamamen sağlayıcıya ait ve öngörülemeyen bir risk olduğundan başka bir kuruluşa transferi çok da anlamlı değildir.
Riskten Kaçınılması: Bulut bilişim kullanan bir kuruluşun bu riskten kaçınması hiçbir zaman tam olarak mümkün değildir.

R.9- Verilerin Güvensiz veya Etkisiz Silinmesi: Müşteri kuruluş sağlayıcılarla sözleşmesini sonlandırdığı durumlarda, verilerinin silinmeme ve ifşa edilme riskine karşı, sağlayıcıları bağlayan maddelerle hizmet seviye anlaşmasını güçlendirmelidir. Bu doğrultuda ilgili riski azaltmak için müşteri kuruluş:

- Sağlayıcının hizmet süresi sonunda, tüm veri ve uygulamalarının tüm kopyalarını kendine teslim edeceğine ve depolama ünitelerinde kayıtlı tüm verileri kalıcı olarak sileceğine dair cezai şart içeren hizmet seviye anlaşması maddesi talep edebilir.
- Verileri kalıcı olarak silinmese dahi, ifşa edilememesi ve herhangi istenmeyen şahıslarca kullanılmaması için, veritabanında etkin bir şifreleme prosedürü uygulatabilir.
- Eğer hizmetleri çok hassas veriler içeriyorsa; sağlayıcının kalıcı olarak veri silme prosedürlerini sağlayan API'lere sahip olduğunu teyit edebilir ve gerektiğinde kullanılmasını şart koşabilir.

- Veri gizliliği konusunda çok hassas veriler içeren uygulamaları için, bu verilerin bağımsız bir fiziksel diskte saklanıp, sözleşme sonunda disk ile birlikte kendisine teslim edilmesi şartını hizmet seviye anlaşmasına ekleyebilir.

Riskin transferi: Müşteri kuruluş tarafından bu risk, sağlayıcının veritabanlarında kendi verileri için etkin bir silme prosedürü uygulayıp uygulamadığının denetimi için bağımsız denetim firmalarına transfer edilebilir ancak bunun için sağlayıcının denetime izin vereceğini ve ilgili kuruluşun verilerini hangi lokasyonlarda barındırdığını sunacağını taahhüt eden bir firma olması gerekir.
Riskten Kaçınılması: Bu riskten tamamen kaçınmak için çok hassas veriler içeren uygulamaları ve bunların yedekleri için müşteri kuruluşlar, bütün verilerinin bağımsız fiziksel disklerde saklanıp, sözleşme sonunda disk ile birlikte kendisine teslim edilmesini talep etmelidir fakat bu durum bulut bilişimin mimarisinin avantajlarının bir çoğunu ortadan kaldırmaktadır.

R.33- Ağ Yönetimi Sorunları: Bu risk çeşitli sebeplerle ağ yönetiminde meydana gelen sorunların, ilgili hizmetin kalitesini ve kullanılabilirliğini ciddi şekilde etkilemesi olup, sıkça meydana gelmektedir. Bu sorunlar ve kuruluş için ortaya çıkardığı risklerin en azından miktar ve etkilerinin azaltılabilmesi için müşteri kuruluş sağlayıcının:

- Yazılım ve firmware güncellemelerini önce test ortamlarında denediğinden ve sonrasında çalışma günlerinin dışında üretim ortamına taşıdığından emin olmalıdır.
- Ağ erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkilerini, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı tutmasını talep etmelidir.
- Ağ erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirdiğini ve kullanıcılar tarafından hizmet için ayrılan tüm internet bant genişliği kaynağının tüketilmesini engellediğini teyit etmelidir (Öztürk, 2014).

- Bütün müşterilerinin yıl içerisindeki ağ bant genişliği kullanım oranlarını ve özellikle de kullanım miktarının en yüksek miktarda gerçekleştiği tarih aralıklarını detaylı bir şekilde istatiksel olarak belirleyerek, müşterilerin herbirine sunduğu bant genişliği kaynağını buna göre optimize etmesini talep etmelidir.
- Kuyruk gecikmesi, paket kaybı ya da yeni bağlantıların engellenmesi gibi ağ yönetim sorunlarını, periyodik olarak kendisine raporlamasını talep etmelidir.
- Müşterilerine ayırdığı bant genişliği kaynağının otomatik kullanıcı talebine göre, hizmet performansını, tepki süresini ve dolayısıyla kullanılabilirliğini düşürmeyecek şekilde artırılabilmesini talep etmelidir.

Riskin transferi: Müşteri kuruluş, ağ trafiği hızının ve buna bağlı olarak hizmetlerinin kalitesi ve kullanılabilirliğinin izlenmesi ve gerekli müdahalelerin yapılması işlerini; bağımsız denetim firmalarına, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devrederek, riski transfer edebilir.
Riskten Kaçınılması: Ağ yönetimi sorunları belli önlem ve kontrollerle azaltılabilir ancak bu sorunlardan tamamen kaçınılması teknik olarak mümkün değildir.

R.3- Servis Sağlayıcı Bağımlılığı: Bu risk, sağlayıcıların müşterilerini kaybetmeme ve yeni rakip firmaların piyasa fiyatlarını düşürmesini önleme amaçlarıyla, kendilerine özel uygulama ve yönetim API'leri geliştirip, standartlara uymama konusunda direnmeleri sonucu ortaya çıkmaktadır. Bu sebeple müşteri kuruluşların, bulut bilişimin farklı servis modelleri için gereksinimlerine uygun sağlayıcı seçmeleri kritik bir öneme sahiptir. Bu sebeple servis sağlayıcı bağımlılığı riskini azaltmak için müşteri kuruluşlarca:

- Hizmet seviye anlaşmalarında sağlayıcıların sundukları taahhütler ve özellikle de başka sağlayıcıya veri aktarma kabiliyeti ve anlaşma sonunda veri ve uygulamaların ne şekilde dışarı taşınıp, kuruluşa iade edileceği bölümleri, kuruluş politikalarına uygun bir şekilde açıkça belirlenmelidir.

- Depolama Ağları Endüstrisi Birliği (SNIA) tarafından oluşturulan Bulut Veri Yönetimi Arabirimi (CDMI) standardı gibi gelişmekte olan bilişim endüstrisi standartlarını destekleyen sağlayıcılar seçilmelidir (Rouse, 2014b).
- Web servis platformları arasında birlikte çalışabilirliğe imkân veren WS-I gibi servis platformu ara yüzlerine sahip sağlayıcılar tercih edilmelidir.
- Uygulama-servis platformu arayüzleri için, sağlayıcıdan bağımsız programlama arayüzleri sunan bulut platformları kullanılması talep edilmelidir. Herhangi bir programlama dilinden bağımsız, standart bir bulut uygulama platformu arayüz yazılımı hizmet seviye anlaşmasında tanımlanmalıdır.
- Yapılan hizmet tanımlarında, hizmetin tüm özelliklerini kapsayan, kolayca okunup, anlaşılabilen hizmet açıklamaları bulunmalıdır.
- Sağlayıcı hizmet yönetim arayüzleri için, sağlayıcıların yeni oluşturulan veya güncellenen standartları (DMTF Bulut Altyapı Yönetim Arabirimi (CIMI) ve Sanallaştırma Yönetimi (VMAN) standartları, Bulut Uygulamaları için OASIS Topolojisi ve Düzenleme Özelliği (TOSCA), Açık Grid Forumu Açık Bulut Bilişim Arabirimi (OCCI) ve SNIA Bulut Veri Yönetimi Arabirimi (CDMI) vb.) takip edip etmediği araştırılmalı ve takip eden sağlayıcılar tercih edilmelidir.
- Kullanılan veri modelleri, metin ve uygulanabilir şema standartlarının (iyi düzenlenmiş XML şemaları) sağlayıcı tarafından açıkça tanımlanması istenmelidir.
- Bulut uygulama bileşenlerinin, etkileşim içerisinde oldukları diğer uygulama bileşenleri ile gevşek bağlı olması aranmalıdır.
- Sağlayıcıların sundukları uygulamaları pazarladıkları online platformlar için gerekli standartları belirlemek ve kuruluşun bulunduğu ülke mevzuatlarına uygun şekilde işletmek konusunda çalışma yapmaları talep edilmelidir.
- Sağlayıcı uygulamalarının *Temsili Durum Aktarımı (REST) dağıtık sistem tarzı kullanılarak dizayn edildiği teyit edilmelidir.
- Standart makine imaj formatları, farklı altyapı hizmet sağlayıcıları ve aynı

Temsili Durum Aktarımı (REST): Web protokolleri ve teknolojilerini kullanan bir dağıtık sistemdir.

sağlayıcının farklı altyapı servisleri arasında olası taşınabilirliği mümkün kılacağından; Açık Sanallaştırma Biçimi (DMTF OVF) standardının sağlayıcı tarafından desteklenmesi şartı aranmalıdır (McKendrick, 2013b).

Riskin transferi: Müşteri kuruluş, sağlayıcı bağımlılığı riskini azaltmaya yönelik ilgili kontrol ve önlemlerle çözüm bulamazsa, bu riski bulut aracılarına devredebilir. Bulut aracıları veri barındırılması, uygulama ve yazılımların işletilmesi, izlenmesi, kontrolü ve yönetimi için açık standartlar (örn. OVF (11)) sunan sağlayıcı firmalarla çalışarak, riski önemli düzeyde minimize edebilir.

Riskten Kaçınılması: Bulut sağlayıcı bağımlılığı, ilgili standartları takip eden sağlayıcılarla çalışılarak azaltılabilir ancak farklı bulut mimarileri ve hizmet modellerinde birçok bağımlılık sebebi ortaya çıkabileceğinden; tam olarak kaçınılması mümkün değildir.

R.15- Hizmet Kesintisi veya Bozulması: Sağlayıcı hizmetinin kesilmesi, özellikle sağlayıcı altyapısı üzerinden kendi kullanıcılarına hizmet veren kuruluşlar açısından ciddi kayıplara yol açabilecek olup; ilgili kesintilerin etkilerini azaltmak için müşteri kuruluşlar:

- Servis sağlayıcı hizmetinin, kesintileri sınırlandırmak için yeterli kapasite ve çoklu servis kaynakları ile tasarlanmasını, sağlayıcı seçiminde tercih sebebi yapmalıdır.
- Sağlayıcıyla, kabul edilemeyecek kadar düşük kullanılabilirlik performans düzeyleri için, caydırıcı cezalar içeren bir hizmet seviyesi anlaşması imzalamalıdır.
- Tanımlanan kullanılabilirlik düzeylerinin, kendi iş amaçları için kabul edilebilir düzeyde olmasını talep etmelidir.
- Servis sağlayıcının aktif bir yedekleme programına ve kurtarma planına sahip olmasına dikkat etmelidir.
- Servis sağlayıcı kurtarma planının düzenli olarak test edildiğini onaylamalıdır.

- Hizmetin kullanılabilir olmadığı durumlarda, alternatif servis seçeneklerinin geçerli olup olmadığını belirlemelidir.
- Bir kesintisi sırasında hizmetler için uygun ve uygulanabilir alternatifleri uygulamalıdır (Mosher, 2011).

Riskin transferi: Hizmet kesintisi veya bozulması riski, sağlayıcıların çoklu servis kaynaklarının temini, gerekli yedekleme ve kurtarma mekanizmalarının tesisi ve uygulanması gibi sorumluluklarının takibi ve gerekli müdahalelerin yapılması amacıyla, bulut aracılarına transfer edilebilir.

Riskten Kaçınılması: Müşteri kuruluş, bu riskten kaçınmak için, bulut servislerini sadece hizmet kesintisi veya bozulmasının kritik sorunlar oluşturmayacağı uygulamaları için kullanabilir veya başka bir servis sağlayıcıdan, gerektiğinde bu hizmeti sürdürecek alternatif bağlantı hatları temin edebilir.

R.10- Nakil Halindeki Veriyi Yakalama: Bulut mimarileri, çok fazla sayıda müşterinin aynı anda veri alış-verişi sağladığı, yönetilmesi zor mimarilerdir. Bu mimarilerde sunucu-istemci arasındaki veri alış-verişi sırasında yaşanacak sızmalar ve verilerin iletim halindeyken yetkisiz kişilerin eline geçmesi olasılıklarına karşı, müşteri kuruluş sağlayıcıdan bir takım önlemler almasını talep etmelidir. Bu önlem ve kontrollerle ilgili başlıca örnekler şu şekildedir:

- Müşteri kuruluş, kaynak izolasyon eksikliği sebebiyle yaşanabilecek izinsiz izleme, yan kanal ve veri iletimi tekrarlama saldırıları vb. durumların sağlayıcı tarafından izlenmesi ve bu saldırılarda bulunan müşterilere gerekli yaptırımların uygulanmasını talep edebilir.
- Sağlayıcılar ayrıcalıklı bağlantıları, teknik olarak güvenli kanallar olan SSL, IPSec VPN gibi veri şifrelenmiş ağ protokolleri üzerinden sunmalıdır.
- İnternet üzerinden sağlayıcının herhangi bir bilgisayar ağına erişen kişiler ve/veya kuruluşlar VPN teknolojisini kullanmalıdırlar. Bu sayede ağ üzerinde; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve

sistem devamlılığını sağlanmalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vb. protokollerden birini içermelidir.

- Sağlayıcının ağ cihazlarına ait loglar, network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
- Sağlayıcı bir merkezi kayıt sunucusu ile kayıtlar üzerinde yaptığı analizler doğrultusunda, saldırı ve normal olmayan durumları tespit edip, ihlal durumunda müşteri kuruluşa uyarı göndermelidir (Öztürk, 2014).

Riskin transferi: Bu risk, gerekli güvenlik kontrolleri ve diğer önlemlerle azaltılabilir fakat öngörülemeyen bir risk olduğundan başka bir kuruluşa transferi çok da anlamlı değildir.

Riskten Kaçınılması: Bulut bilişim kullanan bir kuruluşun bu riskten kaçınması hiçbir zaman tam olarak mümkün değildir.

R.21- Mahkeme Celbi ve E-Keşif: Bulut müşterisi kuruluşların, sağlayıcıların hizmetlerini kullanma amacıyla sözleşme imzalamadan önce, dikkat etmeleri gereken en önemli noktalardan biri de; bulut ortamındaki verilerine sadece kendi değil, bir yasal soruşturma veya e-keşif sebebiyle yargı organları tarafından ihtiyaç duyulabileceğidir. Yine kendisiyle aynı fiziksel kaynağı kullanan başka müşteriler hakkındaki soruşturmalar nedeniyle ilgili fiziksel kaynağa el konulması, kendi hizmetlerini de durdurabilecektir. Bu riskleri azaltmak için müşteri kuruluş:

- Servis sağlayıcının, kendi verilerini içerebilecek herhangi gerekli bir yasal açıklamanın durumunu bildirme konusunda sözleşmeyle bağlı olduğundan emin olmalıdır.
- Böyle bir durumda, e-açıklama (keşif) ihtiyaçlarını karşılayabilmek için iç planlar yapmalıdır (Mosher, 2011).
- Sağlayıcıya, verilerin ömrünü kapsayacak şekilde veri barındırma politikaları uygulamayı, hizmet seviye anlaşmasında şart koşmalıdır.

- Sözleşme oluştururken; kayıt yönetimi, saklama protokolleri ve veriler tutulma biçimi gibi konuları öngören durumlar için, sağlayıcı ile müzakere etmelidir.
- Kendisiyle aynı fiziksel altyapıyı kullanan diğer müşterilerin verileriyle ilgili yasal organların el koyma taleplerinin kendi verilerini etkilememesi için, ilgili müşteri verileriyle kendi verileri arasında gerekli izolasyon ve bölümlendirmelerin (segmentasyon) sağlanmasını talep etmelidir.
- Eğer yeterli izolasyon ve bölümlendirme yoksa, kendisiyle aynı fiziksel altyapıyı kullanan diğer müşterilerin verileriyle ilgili yasal organların el koyma taleplerinin kendi verilerini etkilememesi için, sağlayıcının yeterli yedekleme mekanizmasına sahip olduğunu teyit etmelidir.
- Kolluk kuvvetleri veya sivil görevliler tarafından mahkeme celbi sonucu sağlayıcının fiziksel donanımına el konulması durumunda; verilerini açık veya hibrit bulut mimarilerinde barındırarak, kendi kullanıcılarının yasal haklarını ihlal edip etmeyeceğini irdelemelidir.

Riskin transferi: Bu riskin olası etkileri, uygun saklama protokolleri ve yedekleme mekanizmalarının uygulanması/uygulatılması şartıyla, bir ölçüde bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devredilebilir.

Riskten Kaçınılması: Bulut mimarisinde ve ayrıca geleneksel mimarilerde veri barındıran kişi ve kuruluşlar için, verileri herhangi bir yargılama için dava konusu olabileceğinden bu riskten kaçınmak mümkün değildir.

R.22- Veri sansürü: Bulut sağlayıcıların, özellikle sözleşmelerini kendi lehlerine maddelerle detaylandırmayan müşterilerinin verilerini sansürlemesi veya keyfi şekilde denetlemesi; azaltılması ve önlenmesi diğer birçok riske göre kolay bir risktir. Bu riski azaltmak için müşteri kuruluş,

- Sözleşmeyle servis sağlayıcının bu tür denetleme veya sansürleme faaliyetlerinin kapsamını ve hangi şartlarda yapabileceğini tanımlamalıdır.
- Eğer bu mümkün değilse, bu tür faaliyetlerin servis sağlayıcı tarafından kendisine rapor edilmesini talep etmelidir.

- Söz konusu veri ister kendi yüklediği veri, isterse de sağlayıcının platformu veya uygulaması kullanılarak üretilen veri olsun, her durumda veri sahibinin kim olduğu, kullanma ve değiştirme hakkının kime ait olduğu hususları açıkça hizmet seviye anlaşmasında belirlenmelidir.

Riskin transferi: Bu risk keyfi veri denetimi ve sansürü uygulayan sağlayıcılardan hizmet temin edilmemesi amacıyla, piyasadaki ilgili sağlayıcıların prosedürlerini yakından takip eden bulut aracılarına devredilebilir.

Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluşlar, verilerine ve uygulamalarına denetim ve sansürler uygulayan sağlayıcıların kaynaklarını kullanmayabilirler.

R.28- Sosyal Mühendislik Saldırıları: Sosyal mühendislik saldırıları, geleneksel bilişim mimarilerinde olduğu gibi, bulut bilişimde de hem müşteri kuruluş ve hem de sağlayıcı tarafında çeşitli doandırıcılık yöntemleri kullanarak; kullanıcıların hesap bilgilerine ve özellikle de şifrelerine erişme yoluyla ciddi riskler oluşturmaktadır. Kullanıcıların bu saldırı yöntemleri konusunda farkındalıklarının artırılması yönünde alınabilecek tedbirler, doğal olarak bu saldırıların başarı oranını azaltacaktır. Bununla birlikte bu riski azaltmak için müşteri kuruluş ve sağlayıcıların kullanıcıları,

- Kurumsal verilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek, hiçbir şart altında verilerini ve kullanıcı şifrelerini paylaşmamalıdırlar.
- Sistemde oluşturdukları dosyalara erişecek kişileri ve bu kişilerin haklarını "bilmesi gereken" prensibine göre belirlemelidirler.
- Erişecek kişilerin haklarını yazma, okuma, değiştirme ve çalıştırma yetkilerini göz önüne alarak oluşturmalıdırlar.
- Verilen hakları belirli zamanlarda kontrol etmeli, değişiklik gerekiyorsa yapmalıdırlar.
- Eğer paylaşımlar yapıyorlarsa, ilgili dizine sadece gerekli haklar vermelidirler.

- Sosyal medya hesaplarına giriş için kullandıkları şifreler ile kurum içinde kullanılan şifreleri farklı tutmalı ve kuruma ait hiçbir gizli bilgiyi ve yazıyı sosyal medyada paylaşmamalıdırlar (Öztürk, 2014).
- Zararlı yazılımların bilgisayarlarına yüklenme riskine karşı, güvenliğini teyit etmedikleri flash bellek, harici hard disk gibi depolama cihazlarını bilgisayarlarına takmamalıdırlar.
- Telefon, sesli yanıt sistemi veya e-posta yoluyla kimlik avlama riskine karşı, şifre ve kişisel bilgilerini kesinlikle bu platformlarda paylaşmamalıdırlar.
- Bilgisayarlarında filtreleme, anti-virüs ve güvenlik duvarı yazılımlarını bilinçli bir şekilde kullanmalıdırlar.
- Kimlik ve giriş kartlarını başkalarının erişebileceği yerlere bırakmamalıdırlar.

Riskin transferi: Sosyal mühendislik saldırı riski, tamamen sağlayıcı ve müşteri kuruluşun kendi personelinin kötü niyetli kişilerce kullanılması esasına dayandığından ve bu amaçla çok farklı yöntemler kullanıldığından transferi mümkün değildir.

Riskten Kaçınılması: Sosyal mühendislik saldırıları sağlayıcı veya müşteri kuruluşun personelinin zafiyetlerinden faydalanılmasına dayandığından, bu riskten tamamen kaçınılması mümkün değildir.

R.8- Dış Kaynaklı Saldırılar: Çok fazla sayıda ve disiplindeki müşterilerin aynı ortamda bulunduğu, kontrolü ve işletmesi zor bir mimari olan bulut bilişim, kötü niyetli erişim denemelerinin sıkça yaşandığı bir ortamdır. Bu durumun sağlayıcıların bu saldırılar konusundaki tecrübesini artırıp, veri güvenliği konusunda önemli yatırımlar yapmalarını teşvik etmesi; bulut bilişimi geleneksel mimarilerden daha güvenli hale getirmiştir. Ancak sadece siber güvenlik yatırımları, zararlı faaliyetlerin engellenmesi için yeterli olmamakta olup, bulut mimarisi paydaşlarının sıkı bir bilgi güvenliği politikası uygulayarak, gerekli risk azaltıcı önlem ve kontrolleri uygulaması gerekmektedir. Bu kapsamda aşağıdaki önlem ve kontroller bu riskin azaltılması açısından fayda sağlayacaktır:

- Kuruluş, servis sağlayıcının web uygulamasının geliştirilmesi ve kodlama için önerilen ve her düzeydeki altyapısında kod değerlendirmeleri ve uygun uygulama güvenlik adımları içeren, güvenlik açığı ve penetrasyon testlerini en iyi şekilde takip ettiğini teyit etmelidir.
- Kuruluş, servis sağlayıcının güvenlik açığı ve penetrasyon testlerini periyodik olarak gerçekleştirdiğini ve tanımlanan sorunları düzelttiğini onaylamalıdır.
- Kuruluş, bu uygulamaların denetlenmiş, yerinde ve operasyonel anlamda etkili olduğunu onaylamalıdır (Mosher, 2011).
- Sağlayıcı hizmet sunucularına kullanıcı erişimi için SSH, RDP gibi protokollerle ve sunucu yönetimi için belirli portlara erişim verilmelidir. Yine sunucuların kendi aralarındaki servis ve yönetimleri için belirli portlarla erişim sağlanmalıdır.

Hem müşteri kuruluş ve hem de sağlayıcı tarafında,

- Erişim sağlanacak sunuculara; admin/root yetkili yönetici kullanıcıların, sudo ve runas yetkili kısıtlı yönetici kullanıcıların ve dış dünyadan erişen gibi uygulamayı kullanan kullanıcıların farklı ayrıcalıklarla erişimi sağlanmalıdır.
- Parola yönetimi ile ilgili, parola yönetim politikaları oluşturulmalıdır.
- Kullanıcılara sunucu yönetimi için sağlanan erişimde, admin/root yetkisi sistem grubu dışında tanımlanmamalıdır.
- Sunucu servislerinin yönetim işlemlerinde, yetkili kullanıcı bilgileri sistem grubuna teslim edilmelidir. Sunucu servislerinin yönetim işlemleri, merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır (Öztürk, 2014).

Riskin transferi: Dış kaynaklı saldırı riski müşteri kuruluş tarafından, bilgi güvenliği ile ilgili gerekli prosedürlerin uygulanması ve dış kaynaklı tehditlere karşı topyekün kontrolün sağlanması amacıyla Siber Güvenlik Operasyon Merkezleri'nin kurulması ve işletilmesi şartıyla, bulut sağlayıcısı üst kuruluşlara devredilebilir.

Riskten Kaçınılması: Dış kaynaklı saldırı riskinden, gerek bulut ve gerekse de geleneksel bilişim mimarilerinde tam olarak kaçınılması mümkün olmamakta ancak azaltıcı kontrol ve önlemlerle olasılığı ve etkileri minimize edilebilmektedir.

R.19- Hizmet Motorunun Hacklenmesi: Sanallaştırmaya dayalı bir mimari olan bulut bilişimde, bu ortamı yöneten hipervizörlerin güvenliği son derece önemlidir. Hipervizörlerde meydana gelebilecek her türlü başarılı kötü amaçlı aktivite, bütün sanal makinelerde yüklü veri ve uygulamaları risk altına sokacaktır. Bu riskleri azaltmak için hipervizör güvenliğiyle ilgili müşteri kuruluş sağlayıcıdan:

- Mümkün olduğunca az miktarda kod, disk kaplama alanı ve az sayıda arayüze sahip fonksiyonel bir hipervizör yönetim konsolu ile daha az saldırı yüzeyi sunmasını talep edebilir.
- Sertifikalı olmayan sürücülerin kullanılmasına izin vermemek için, hipervizörlerin ön yükleme yapılandırma seçeneğinin olmasını talep etmelidir.
- Tüm sanal makinelerin toplam yapılandırılmış belleğinin, sanal ana RAM belleğine oranının çok yüksek olmamasını isteyebilir (1,5/1 idealdir).
- Sanal makine görüntü kütüphanesinin, hipervizör konağın dışında ikamet etmesini ve kütüphaneden kontrol edilen her görüntünün özgünlük ve bütünlüğü için ona bağlı bir dijital imzanın olmasını talep edebilir.
- Sanal makine hizmetleri için, izleme ve güvenlik politikasının uygulanmasını ve bu sayede sanal makinlerin içindeki ve sanal makinelere giriş ve çıkış yapan kötü niyetli trafiğin izlenmesini ve bertaraf edilmesini talep etmelidir.
- Hipervizörlere doğrudan erişim sağlayabilen kullanıcı hesaplarının sayısının mümkün olduğunca az sayıda olmasını istemelidir.
- Sağlam kimlik doğrulama protokolleri yoluyla kimlik doğrulamasını etkinleştirmek, güvenlik politikalarının uygulanmasını sağlamak ve kullanıcı hesabı listesindeki değişikliklere uyum sağlamak için, hipervizör host üzerindeki kullanıcı hesaplarının, kurumsal dizin altyapısı ile entegre edilmesini talep etmelidir.

- Hipervizör servis konsoluna erişim için kullanılan uzaktan erişim protokolünün; erişimi tamamen reddetmek, hipervizör root hesabı erişimini reddetmek veya sadece idari hesapların belirli bir listeye erişimini kısıtlamak gibi yapılandırma seçenekleri olmasını istemelidir.
- Etkin bir hipervizör yama yönetimi uygulamasını ve hipervizörü güncel tutmak için ilgili tüm yamaların sağlanmasını talep etmelidir.
- Hipervizör için yerleşik güvenlik duvarının sadece hipervizör içindeki; yönetim, uzman güvenlik ve üçüncü parti uygulamaları gibi etkin hizmetler için ihtiyaç duyulan bağlantı noktalarına ve protokollere izin verecek şekilde yapılandırılmasını talep etmelidir (Chandramouli, 2014).

Riskin transferi: Hizmet motorları sağlayıcıların işlettiği platformlar olup, bu platformlarla ve özellikle de hipervizörlerle ilgili kontrol ve yönetim sorumluluğu sağlayıcıya aittir. Müşteri kuruluş, sağlayıcıyla yaptığı hizmet seviye anlaşmasında, hizmet motoru yönetim prosedürlerini belirtmek ve sağlayıcıyı bunlara zorlamak yoluyla riski azaltabilir ancak bir başka kuruluşa devredemez.

Riskten Kaçınılması: Bulut bilişim, fiziksel donanım kaynakları üzerinde çalışan ve müşteri kaynaklarını farklı veri soyutlama düzeylerinde yöneten, son derece uzmanlaşmış platformlar olan hizmet motorlarına bağımlı olduğundan, bu riskten kaçınılması olası değildir.

R.27- Ağ Kesilmeleri: Ağ kesintisi riski tüm bulut hizmetlerini durduracağından bu riskin gerçekleşme sayısını ve ağda yaşanan kesintinin süresini azaltmak için müşteri kuruluş,

- Sağlayıcıdan, fiziksel sebeplerle ağ kesintilerinin yaşanmaması için; ağ cihazlarının sistem odası gibi yerlerde şifreli kabinlerde konumlandırılması ve sistem odası dışında kalan cihazların da yine uygun kabinlerde kapalı dolap ya da şifreli kabinlerde korunması gibi gerekli fiziksel önlemlerin alınması ve ağ fiziksel kaynaklarının yedekli olarak sunulmasını talep etmelidir.

- Sağlayıcıdan, eneri kesintileri sebebiyle ağ kesintilerine karşı, ağ cihazlarını yedekli UPS prizleri üzerinden beslemesini talep etmelidir.
- Sağlayıcıdan, ağ cihazlarının IP ve MAC adreslerinin düzenli bir şekilde tutulması, cihazlara sadece yetkili kişilerin erişebilmesi için parola ve kullanıcı ayrıcalık politikaları belirlenmesi, cihazların kullanılmayan servislere kapatılması, yönlendirici ve anahtarların kontrolünün ağı yöneten personelin kontrolünde olması gibi önleyici çalışmaları talep etmelidir.
- Sağlayıcının hizmetlerine erişen cihazları bir yönetim yazılımı ile devamlı olarak gözlemlediğini teyit etmelidir.
- Sağlayıcının hizmetlerine erişen cihazların firewall üzerinden ağa dâhil olmasını ve sağlayıcının kendi iç kullanıcı bilgisayarlarında kişisel anti-virüs ve güvenlik duvarı yazılımlarının yüklü olmasını talep etmelidir (Öztürk, 2014).

Riskin transferi: Müşteri kuruluş, ağ kesintilerine karşı hizmetin mevcut ağdan bağımsız yedek başka bir ağ altyapısından sürdürülmesi talebiyle, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına bu riski transfer edebilir.

Riskten Kaçınılması: Ağ kesintileri fiziksel sebepler, enerji kesintileri veya kötü niyetli aktiviteler gibi birçok sebebe bağlı olabilen riskler olup; bu risklerden tamamen kaçınılması olası değildir.

R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması: Bulut sağlayıcısı firmanın devri, şirket birleşmesi vb. ticari anlaşmalar neticesinde, yeni hizmet sağlayıcının hizmetler için kendi arayüzlerini veya güvenlik kontrollerini kullanmak istemesi; özellikle yeni hizmet sağlayıcısı piyasada faaliyet gösteren bir firmaysa olası bir durumdur. Bu sebeple, müşteri kuruluşun satın aldığı hizmetin tüm ayrıntılarıyla sözleşme ve eklerinde yer alması gerekmektedir. Bu kapsamda müşteri kuruluş sağlayıcı firmanın el değiştirmesi durumunda:

- Sağlayıcı ile imzalanan sözleşmenin koşullarının, belirtilen sözleşme süresi boyunca aynen geçerli olacağını kayıt altına aldırmalıdır.

- Kullanılacak uygulama, izleme, yönetim ve kontrol arayüzleri ve diğer API'lerin aynen aynen devam ettirilmesini veya en azından kuruluşun kendi hizmetleriyle uyumlu olmasını talep etmelidir.
- Hizmet altyapısı için uygulanacak güvenlik kontrolleri ve güvenlik ile ilgili diğer yatırımların aynı şekilde sürdürüleceğini teyit etmelidir.
- Hizmet kullanılabilirliği ve kalitesinin, asgari önceki sağlayıcının sunduğu düzeyde olacağını talep etmelidir.

Riskin transferi: Bulut sağlayıcısı firmanın el değiştirmesi, olağan fakat öngörülebilecek bir durum olmadığından riskin transferi mümkün olmamaktadır.

Riskten Kaçınılması: Sağlayıcı firmanın el değiştirmesi durumunda yaşanacak risklerin dereceleri uygulanacak önlem ve kontrollerle azaltılabilir fakat tam olarak kaçınmak mümkün değildir.

R.12- Kaynak Tükenmesi: Bulut sağlayıcıların kaynak tedariği konusunda öngörü ve modellemelerinin başarısızlığa uğraması sonucu, müşterilerinin ihtiyaçlarına cevap verme konusunda yetersiz kalması riskinin önüne geçmek için, hizmet seviye anlaşmasında bu konuda düzenlemelerin yapılması gerekmektedir. Bu amaçla müşteri kuruluş:

- Hizmet seviye anlaşmasında gerçekçi bir kaynak artırım limiti belirterek, gerektiği takdirde asgari bu kaynağın tedarik edilmemesi itimaline karşı cezai şart koşmalıdır.
- Sağlayıcının kendi kaynağının yetersiz kaldığı durumlarda, başka sağlayıcılardan veya alt yüklenicilerden kaynak tedarik edebilme durumunu teyit etmelidir.
- Sağlayıcının temin ettiği kaynaklarını etkili bir biçimde izlediğinden ve kaynak yetersizliğine karşı gerekli altyapı yatırımlarını yaptığından emin olmalıdır.

Riskin transferi: Bu risk müşteri kuruluş kaynak talebinin sürekli kontrol edilerek, yedek kaynak miktarının belli limitlerin altına düşmesi durumunda, başka sağlayıcı veya alt yükleniciden kısa sürede kaynağın temin edilmesi talebiyle; bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına bu riski transfer edilebilir.

Riskten Kaçınılması: Her ne kadar sınırsız kaynak sunuyor hissi yaratsa da, bulut bilişimde kaynak tükenmesi riski mevcut olup, yedek kaynak tedariği ile azaltılabilecek bu riskten tam olarak kaçınmak olası değildir.

R.16- Kötü Amaçlı Araştırma Veya Taramalara Girişilmesi: Sağlayıcı veya müşteri kuruluş alt yapısındaki güvenlik açıklarını tespit ve istismara dayalı girişimlere karşı, çeşitli bilgi güvenliği kontrol ve önlemleri uygulanabilir. Bu doğrultuda riski azaltmak için müşteri kuruluş,

- Üçüncü taraf sağlayıcı çözümünde, yalnızca gerekli ve hassas olmayan verileri barındırabilir.
- Bulut çözümlerinde barındırdığı verileri şifreleyerek aktarabilir.
- Başka bir sağlayıcının çözümü veya kuruluşun iç kaynakları üzerinden, hizmetlerin devamlılığını sağlayacak bir yük devretme stratejisi oluşturabilir (Horwath, 2012).
- Sağlayıcıdan böyle ihlal durumlarında, derhal kendi sistem yöneticilerini haberdar etmesini ve gerekli ihlal bildirimlerini sağlamasını sözleşmeye ekleyerek talep etmelidir.
- Sağlayıcının dış dünyadaki sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portlarını özel durumlarda açtığını teyit etmelidir.
- Sağlayıcının, sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle ve sunucu yönetimi için belirli portlara erişim verdiğinden ve yine sunucuların kendi aralarındaki servis ve yönetimleri için belirli portlarla erişim sağladığından emin olmalıdır (Öztürk, 2014).
- Servis sağlayıcının, web uygulamasının geliştirilmesi ve kodlama için önerilen ve her düzeydeki altyapısında kod değerlendirmeleri ve uygun uygulama güvenlik adımları içeren, güvenlik açığı ve penetrasyon testlerini en iyi şekilde takip ettiğini teyit etmelidir.
- Sağlayıcı ve kendi iç kullanıcılarına ait bilgisayarlarda, kişisel anti-virüs ve güvenlik duvarı yazılımları yüklü olduğunu teyit etmelidir.

Riskin transferi: Bu risk müşteri kuruluş tarafından bilgi güvenliği ile ilgili gerekli prosedürlerin uygulanması ve dış kaynaklı tehditlere karşı topyekün kontrolün sağlanması amacıyla, Siber Güvenlik Operasyon Merkezleri'nin kurulması ve işletilmesi şartıyla, bulut sağlayıcısı üst kuruluşlara devredilebilir.

Riskten Kaçınılması: Bu riskten, gerek bulut ve gerekse de geleneksel bilişim mimarilerinde tam olarak kaçınılması mümkün olmamakta ancak azaltıcı kontrol ve önlemlerle olasılığı ve etkileri minimize edilebilmektedir.

R.23- Lisans Riskleri: Lisans riskleri, hem kullanıcının hizmet aldığı sanal makine başına ücretlendirilmesi ve hem de bulutta kendi geliştirdikleri uygulama ve yazılımların fikri mülkiyet haklarına aykırı kullanılması durumları için geçerlidir. Bu riskleri azaltmak için müşteri kuruluş:

- Kullandığı yazılımlarda lisans ücretlerinin ne şekilde belirlendiğinin farkında olmalı ve özellikle kaynak kullanımı artışlarında, her yeni sanal makine başına ayrıca yeni yazılım lisansı ücretleri ödememek için hizmet seviye anlaşmasında gerekli önlemi almalıdır.
- Sağlayıcı ortamında yazılım veya uygulama geliştirmesi durumunda, kendi özgün çalışmasının izinsiz kullanılmaması için her türlü haklarının kendisine ait olduğunu açıkça belirtmelidir.

Riskin transferi: Ek lisanslama ücretleri sebebiyle maliyet artışı ve müşteri kuruluşun geliştirdiği özgün yazılımların kullanılması riskleri, sözleşmelerin bu konularda detaylandırılması yoluyla azaltılabilecek riskler olup, transfer edilmesine gerekli değildir.

Riskten Kaçınılması: Bu risklerden tamamen kaçınmak için, ek lisans ücreti ödemelerinin yapılmayacağı ve müşteri kuruluşların özgün yazılımlarının izinsiz kullanılmayacağı konularının sözleşmeyle taahhüt altına alınması gerekmektedir.

R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı: Aynı altyapıyı paylaştığı diğer müşterilerin faaliyetleri nedeniyle zarara uğrama riski, özellikle sanallaştırma teknolojisinin artırdığı bir risktir. Müşteri kuruluşlar bu riski azaltmak için:

- Sağlayıcıdan, farklı kuruluşların veri ve uygulamaları arasında iç engeller ve bölümlemeler (segmentasyon) uygulamasını talep etmelidir.
- Sağlayıcının kendisiyle aynı altyapıyı kullanan diğer müşterileri spam gönderme, port tarama, kötü amaçlı içerik sunumu gibi faaliyetlerine karşı izlendiğinden, gerekli tedbirleri alıp yaptırımları uyguladığından emin olmalıdır.
- Başka kullanıcıların zararlı faaliyetleri sebebiyle kendi hizmetlerinin engellenmesi veya fiziksel doanıma el konulması durumlarına karşı sözleşmeye cezai şart eklemelidir.
- Kendi uygulamalarının, kurumsal niteliğe sahip veya zararlı faaliyet gerçekleştirme riski düşük müşteri profili bulunan kullanıcılarla aynı fiziksel altyapıda barındırılmasını talep edebilir.
- Bu sebeple yaşayabilecekleri veri kaybı için, yeterli yedekleme prosedürünün uygulandığını teyit etmelidirler.

Riskin transferi: Müşteri kuruluşun bu riski herhangi bir sağlayıcı üst kuruluşa veya bulut aracısına transferi olası değildir. Ancak yukarıda belirtilen kontrol ve önlemlerin uygulaması yoluyla risk önemli ölçüde azaltılabilir.

Riskten Kaçınılması: Bu riskten kaçınmak için müşteri kuruluş sağlayıcıdan sadece kendi uygulama ve verilerine adanmış bağımsız fizksel kaynaklar talep edebilir ancak bu durum bulut bilişim mimarisinin faydalarını önemli ölçüde işlevsiz kılmaktadır.

R.18- Şifreleme Anahtarlarının Kaybı: Veri güvenliği ve gizliliği için şifrelemenin hayati önem taşıdığı bulut bilişimde, zaman içerisinde çok büyük sayılara ulaşan şifreleme anahtarlarının yönetimi kritik bir konudur. Bu anahtarların kaybının verilerin geri döndürülemeyecek şekilde kaybedilmesine yol açacabileceği düşünüldüğünde; yönetim ve muhafazalarının uygun şekilde yapılmasının ne kadar önemli olduğu ortaya çıkmaktadır. Bu amaçla, riski azaltmak için müşteri kuruluş:

- Kriptografik anahtarların korunması ve şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetiminin, sağlayıcı tarafından uygulandığını teyit etmelidir.
- İlgili politikanın uygulanması için, sağlayıcı tarafında, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlendiğini onaylamalıdır.
- Anahtar yönetimi ile ilgili olarak sağlayıcının; farklı kriptografik sistemler ve farklı uygulamalar için anahtar üretimi, açık anahtar sertifikası üretimi ve elde edilmesi, anahtarın alınmasını müteakip nasıl faaliyete geçirileceği dâhil kullanıcılara anahtar dağıtımı, yetkili kullanıcıların anahtarlara erişiminin sağlanmasını da kapsayan anahtarların saklanması, anahtarların ne zaman ve nasıl değiştirileceğinin kurallarını da kapsayan anahtarların değişimi ve güncellenmesi, güvenliği tehlikeli bir duruma düşmüş anahtarlar, anahtarların geri alımı ve kullanılmaz hale getirilmesini kapsayan anahtarın yürürlükten kaldırılması, iş süreklilik yönetiminin bir parçası olarak kaybolan veya bozulan anahtarların kurtarılması, anahtarların arşivlenmesi, anahtarların imhası, anahtar yönetimi ile ilgili faaliyetlerin izleme kayıtlarının (log) tutulması gibi konularda aldığı aksiyonları incelemeli ve uygunluğunu teyit etmelidir.

Riskin transferi: Müşteri kuruluş verilerinin hassasiyet seviyelerine göre şifreleme anahtar yönetimi görevini, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına sözleşmeyle devrederek, şifreleme riskini belli ölçüde transfer edilebilir ancak özellikle hassas veriler içeren uygulamaları yöneten kuruluşların şifreleme anahtar yönetimini bizzat uygulaması gerekmektedir.

Riskten Kaçınılması: Bu riskten kaçınmak için, müşteri kuruluşlar bulut servislerini veri gizliliği amacıyla şifrelemesi gereken veriler için tercihen kullanmayabilirler.

R.30- Ağ Trafiğini Değiştirme: İnternet üzerinden sunulan hizmetlere dayalı bulut bilişim mimarisinde, uygulamaların ağ trafiğinde yaşanan değişimlerden asgari düzeyde etkilenmesi ve hizmet kalitesi ve kullanılabilirliğinin idamesi için etkin izleme, kontrol ve yönetim politikalarının geliştirilmesi gerekmektedir. Bu amaçla yaşanabilecek riskleri azaltmak için kuruluş sağlayıcının:

- Ağ trafiğinde anlık yaşanacak değişiklikler ile ilgili bir kontrol, izleme ve yönetim mekanizmasına sahip olduğundan emin olmalıdır.
- Ağ boyunca hizmet performans ve kalitesini idame ettirmek amacıyla, veri ve trafik tiplerinin önem düzeylerini ve buna bağlı ağ kaynağı ihtiyaçlarını belirlemesini talep etmelidir.
- Müşterilerine ayırdığı bant genişliği kaynağının, otomatik kullanıcı talebine göre; hizmetin performansını, tepki süresini ve dolayısıyla kullanılabilirliğini düşürmeyecek şekilde artırılabilmesini talep etmelidir.
- Müşterilerinin kullandığı büyük veri uygulamalarının ve uygulamalara platform bağımsız erişimin ağ trafiğinde yaratacağı dalgalanmaları dengeleyecek ağ yönetimi çözümleri sunmasını talep etmelidir.

Riskin transferi: Müşteri kuruluş, ağ trafiği hızının ve buna bağlı olarak hizmetlerinin kalitesi ve kullanılabilirliğinin izlenmesi ve gerekli müdahalelerin yapılması işlerini bağımsız denetim firmalarına, bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına devrederek, riski transfer edebilir.
Riskten Kaçınılması: Ağ trafiği değişimi riskleri aktarılan verinin türü, aktarım yöntemi, mobil erişim veya kötü niyetli aktiviteler gibi birçok sebebe bağlı olabilen riskler olup; bu risklerden tamamen kaçınılması olası değildir.

R.25- Ayrıcalık Yükseltme Olasılığı: Herhangi bir yazılımın tasarım kusuru veya yapılandırma eksikliği gibi nedenlerle, bir kullanıcının kendisine tanımlanandan daha yüksek ayrıcalıklar elde etmesi durumu; ilgili yazılımın kod geliştirme, derleme, ayrıcalık tanımlama ve menü ekleme işlemlerinde hassas davranılması ve belli önlem ve kontrollerin uygulanması yoluyla olasılığı azaltılabilecek bir risktir. Bu riski azaltmak için müşteri kuruluş ve sağlayıcılar:

- Bulut kaynağı üzerinde uygulama yazılımı geliştirirken veya mevcut yazılım üzerinde değişiklik yaparken, mevcut ayrıcalık ayırma şemasını bozmamaya özen göstermelidirler.

- Geliştirdiği veya temin ettiği kodu mümkün olduğunca yönetici ayrıcalıkları olmadan veya en az ayrıcalıkla çalıştırmalıdırlar.
- Ayrıcalık alanları arasında sıkı bir ayrım yapmalı, eğer mümkünse kullanıcı dizinlerini, diğer kullanıcıların girişlerine engellemeli ve yönetici hesabı giriş menülerini, standart kullanıcı girişlerinden ayırmalıdırlar.
- Zamanında ve etkin güvenlik güncellemeleri yapılan yazılımlar kullanmalı ve böylece yeni ortaya çıkan ayrıcalık yükseltme ile ilgili açıkları belirgin tehlike yaratmadan önleyebilmelidirler (Perrin, 2010).
- Bellekte adresleri bilinen ayrıcalık talimatlarında meydana gelebilecek ara bellek aşmalarını engellemek veya daha zor hale getirmek için, adres alanı sıralamasını rastgele yapmalıdırlar.
- Yazılım geliştirirken arabellek aşmalarını engellemek için derleyici kullanmalıdırlar.
- Yazılımlarını ve yazılım bileşenlerini şifrelemelidirler.
- Zorunlu erişim kontrolleri gerektiren işletim sistemleri kullanmalıdırlar.

Riskin transferi: Ayrıcalık yükseltme hem müşteri kuruluş ve hem de sağlayıcı tarafındaki kullanıcıların karşı karşıya kalabilecekleri bir sorun olduğundan, başka bir kuruluşa transferi olası değildir. Sadece yukarıdaki gibi gerekli kontrol ve önlemler uygulanarak olasılığı azaltılabilir.

Riskten Kaçınılması: Ayrıcalık yükseltme riskleri; kötü niyetli aktiviteler, sosyal mühendislik saldırıları, uygulamaların tasarım ve yapılandırma kusurları gibi birçok sebebe bağlı olabilen riskler olup; bu risklerden tamamen kaçınılması olası değildir.

R.31- Yedeklerin Kaybolması veya Çalınması: Yedekleme hem sağlayıcı ve hem de müşteri kuruluş için; kötü niyetli saldırılar, altyapıdaki fiziksel arızalar, doğal afetler, yazılım ve uygulama sorunları veya yönetici hataları gibi nedenlerle, bozulan ve kullanılmaz hale gelen veri ve uygulamaların tekrar devreye alınabilmesi için, bilişim teknolojilerinde olmazsa olmazdır. Kuruluşların bu tip durumlarda verilerini ve uygulamalarını tamamen kaybetmemek adına, etkili bir yedekleme politikası belirlemesi

ve gerektiğinde uygulaması gerekmektedir. Bu doğrultuda bu riski azaltmak için müşteri kuruluş ve sağlayıcılarca:

- Bilişim politikalarında veri yedeklemesi konusuna mutlaka yer verilmeli ve veri yedeklemesi için yönetim prensipleri ortaya konularak, işlemler bu doğrultuda gerçekleştirilmelidir.
- Yedekleme işlemlerinin sağlanması için, yedekleme politikasına uygun bir yedekleme planı oluşturulmalıdır.
- Yedekleme işlerine ait kayıtlar tutulmalı, başarısız olan yedekleme işleri takip edilerek, yedeği alınamamış verinin yedeği alınmalıdır.
- Yedeklenmiş verilerinin düzenli aralıklarla geri döndürme testleri yapılmalıdır.
- Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır.
- Yedekleme kopyalarının doğru ve tam kayıtları ile dokümante edilmiş geri yükleme süreçleri sağlanmalıdır.
- Yedeklemelernin türü (tam yedekleme/değişen kayıtların yedeklenmesi) ve yedeklemelerinin sıklığı; iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir.
- Yedekleme bilgilerine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır. Herhangi bir tehlike durumunda kullanımını sağlamak maksadıyla, yedekleme bilgisi düzenli olarak test edilmelidir.
- Verilerinin gizliliğinin önemli olduğu durumlarda, yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır.
- Personel güvenliği, bilgi işleme tesisleri ve kurumsal varlıkların korunması garanti altına alınmalıdır.
- İş sürekliliği planları, kabul görmüş iş sürekliliği stratejisi paralelinde ve bilgi güvenliği gereksinimlerine göre formüle ve dokümante edilmelidir.
- Kurtarma ve yeniden başlatmayla ilgili askıda kalan işlerin tamamlanmasını sağlayan operasyonel prosedürler belirlenmelidir.

- Farklı senaryolara göre masa üstü ve teknik kurtarma testleri yapılmalıdır (Öztürk, 2014).

Riskin transferi: Müşteri kuruluş, veri ve uygulama yedeklerinin çalınmasına veya kaybolması riskini sözleşme yoluyla, gerekli fiziksel önlemler ve veri yedeklemesi prosedürlerini uygulamak üzere bulut sağlayıcısı üst kuruluşlara veya bulut aracılarına transfer edebilir.

Riskten Kaçınılması: İlgili kontrol ve önlemlerin uygulanması yoluyla olasılığı azaltılabilecek olan bu risk; kötü niyetli saldırılar, altyapıdaki fiziksel arızalar, doğal afetler, yazılım ve uygulama sorunları veya yönetici hataları gibi birçok nedene bağlı olabileceğinden, tamamen kaçınılması olası değildir.

4.4. Bulut Bilişim Risk İşleme Maliyet Analizi

Risk yönetimi sürecinde tespit edilen risklerin, meydana gelme olasılıklarının ve gerçekleşenlerin kuruluşların faaliyetlerine olan etkilerinin azaltılması amacıyla uygulanan risk işleme sürecinin kritik noktalarından biri de risk işleme maliyet analizidir. Bu süreçte kuruluşlar, tespit ettikleri risk azaltıcı kontrol ve önlemlerin yanısıra, risk işleme yöntemi maliyetinin, sağlanacak faydaya değip değmeyeceğini belirlemelidirler. Bu doğrultuda mali kaynaklarını tahsis ederek, uygun maliyetli kontrolleri uygulamak için, kuruluşlar öncelikle ilgili riske dair olası tüm kontrolleri tespit etmelidirler. Sonrasında her bir kontrol ile ilgili, kontrolün etkinliğine ve mali olarak uygulanabilirliğine dair fayda-maliyet analizi yaparak; hangi kontrollerin kendi durum ve şartları için gerekli ve uygun olduğunu belirlemelidirler. Böylece kuruluşlar, ilgili kontrolün uygulanmasının yaratacağı maliyet kaleminin haklı ve gerekli bir harcama olduğunu kanıtlayabilirler ve az bir maddi fayda sağlayacakları bir işlem için bundan daha fazla ödeme yapmamış olurlar.

Kuruluş tarafından gerçekleştirilen bir fayda-maliyet analizinde, öncelikle yeni geliştirilmiş önlem veya kontrolün uygulanmasının ve uygulanmamasının riske etkisi belirlenir. Burada her iki durum arasında oluşan fark, bu kontrol ve önlemin kuruluş açısından yaratacağı faydayı temsil eder.

İkinci olarak, ilgili kontrol ve önlemin uygulama maliyetinin belirlenmesi gerekir. Bu maliyete etki eden kalemlerden bazıları; donanım ve yazılım teminleri, artan güvenlik gereksinimlerinin sistem performansını veya işlevselliğini azaltmaması için uygulanacak ek politika ve prosedürlerin uygulama maliyetleri, ilgili politika, prosedür veya hizmetleri uygulamak için ek personel istihdam maliyeti, eğitim masrafları ve bakım masrafları olarak sıralanabilir.

Son olarak ilgili kontrol ve önlemlerin uygulanmasının kuruluş için önemini belirlemek için, gerekli maliyetler ve sağlanacak faydalar karşılaştırılır. Eğer kuruluşun iş operasyonları ve bunların kritikliği açısından sağlanacak fayda, harcanacak maliyete göre değerliyse; ilgili kontrolün uygulanmasına karar verilebilir. Burada ilgili kontrolün uygulama maliyetinin yanında, sürdürülme maliyetinin de değerlendirilmesi gerekmektedir. Bu sayede kuruluşlar, ilgili kontrolün standart bir prosedür olarak sürekli uygulanmasına veya aşırı maliyeti göz önüne alınarak uygulanmamasına karar verebilecektir.

Bulut bilişim ile ilgili örnek bir fayda-maliyet analizi aşağıdaki gibi gerçekleştirilebilir:

Kuruluş faaliyetleri ve kişisel veriler açısından kritik ve hassas bilgiler içeren bir uygulamanın, veri iletimi ile ilgili şifreleme kontrolünün etkin olmadığı bir durumu düşünelim. Burada kullanıcılara sunulan hizmetler için, veri aktarımında şifrelemenin kullanılıp kullanılmayacağı kararı; ancak yapılacak olan fayda-maliyet analiziyle verilebilecektir.

Bu analiz için öncelikle şifreleme kontrolünün etkin olduğu ve olmadığı durumlar tartışılır. Bu kapsamda şifreleme özelliğinin etkin olması, müşteri kuruluşun sunduğu uygulamalara ait veriler için daha fazla işlemci gücü harcanmasına, sistem veri aktarım performansının yavaşlamasına ve bu nedenle verimliliğin düşmesine neden olabilecektir. Şifreleme kontrolü yapılmadığı durumlarda ise, nakil halindeki verinin yakalanması gibi kötü niyetli faaliyetler sonucunda, veri güvenliği ve gizliliğinin tehlikeye girmesi olasıdır.

Bu iki durum karşılaştırıldıktan sonra, ilgili uygulamaya şifreleme kontrolü sağlanmasının toplam maliyeti hesaplanmaya çalışılır. Burada toplam maliyetin hesaplanabilmesi için, bu maliyeti etkileyecek kalemler olan; uygulama şifreleme özelliğinin etkinleştirilmesi, şifreleme anahtarı oluşturma ve depolama, şifreleme kontrolünün yütülmesi için ek personel temini, eğitim, bakım ve bunlara ek olarak şifreleme izleme, raporlama ve arşivleme maliyetleri tek tek hesaplanmalıdır.

Bu işlemler sonrasında, kuruluşun misyonu çerçevesinde sorumlu yöneticiler ilgili risk seviyesini belirleyerek, şifreleme kontrolünün kullanılıp kullanılmayacağına karar verebilirler. Bu kapsamda ilgili kontrol sisteme dâhil edilebilir, edilmeyebilir veya ilgili karar daha sonra değerlendirilmek üzere ertelenebilir. Her ne kadar kuruluşların kendi iç operasyonları ve misyonları çerçevesinde, risk değerleri ve ilgili kontrol maliyetleri değişse de; genel olarak ilgili kontrolün uygulanmasında aşağıdaki kurallar geçerlidir:

- Eğer ilgili kontrol riski istenilenden fazla azaltacak olursa, daha ucuz bir alternatif araştırılır.
- Eğer ilgili kontrol, sağlanan risk değeri azaltımının sağlayacağı katkı maliyetinden daha pahalı olursa, başka bir kontrol aranır.
- Eğer ilgili kontrol, riski yeterince azaltmazsa, daha fazla kontrol veya farklı bir kontrol aranır.
- Eğer ilgili kontrol, yeterli miktarda risk azaltımı sağlıyor ve uygun maliyetli ise kullanılır (Stoneburner, 2002).

Artık Risk: Kuruluşlar, yeni kontroller yoluyla, risklerin tehdit olasılıklarının veya iş operasyonlarına etkilerinin azaltılmasını sağlayabilirler. Bu yolla, kullandıkları hizmet servislerinin maruz kaldığı tehdit veya zafiyetlerin bir kısmını ortadan kaldırılabilir veya tehdit kaynağının etki derecesini ve kapasitesini azaltabilirler.

Bu kapsamda geliştirilen risk kontrolleri arasından hangilerinin kullanılacağı ve hangilerinin kullanılmayacağı konusunda seçim yapıldıktan sonra sıra, belirlenen tüm risk kontrollerinin uygulanması aşamasına ve bunun sonrasında da, bir projede veya

faaliyette hâlen varlığını sürdüren artık riski göze alıp almama konusunda verilecek karara gelir. Burada artık risk, iç kontroller uygulanıp gözlemlendikten ve riske etkileri gözden geçirildikten sonraki değiştirilmiş risk olarak tanımlanabilir.

Burada uygulanan kontrol ve önlemler riski tamamen ortadan kaldırabilir veya risk seviyesini sıfıra düşürebilir. Müşteri kuruluşların belirlenen riskleri için uygun kontroller yapıldıktan sonra, sağlayıcılarla bu kuruluşlar arasında, eğer varsa ve göze alınabilecek nitelikteyse artık riski kabul eden ve böylece bulut hizmeti yeniyse başlatılmasına veya varolan bir hizmetse işleyişine devam etmesine karar veren, bir mutabakata varılabilir. Eğer uygulanan kontrol ve önlemler sonucunda, artık risk kabul edilebilir bir seviyeye indirilememişse, bu riski kabul edilebilir bir seviyeye düşürebilmek için risk yönetimi döngüsü tekrar edilmelidir.

4.5. Bulut Bilişimde Risk İzleme ve Değerlendirme

Kuruluşların risk yönetimi süreçlerinin son aşaması, bu sürecin verimliliğini ve etkinliğini belirleyen en önemli faktörlerden biri olan risk izleme ve değerlendirmedir. Bu aşama ile ilgili süreç belirlenip, süreklilik arz eden bir şekilde uygulandığı takdirde; risk yönetimi eylem planları sürekli güncelliğini ve etkinliğini muhafaza edebilecektir. Günümüzde ortaya çıkan yeni teknolojiler ve modern yaklaşımlar sonucu sürekli değişen iş ortamlarında, kuruluşların karşı karşıya kaldığı risklerin olasılıklarının ve etkilerinin, uygulanan iş modelindeki değişikliklere bağlı olarak değişmesi kaçınılmazdır. Burada risk önemli ölçüde değişmiş ve böylece geçerli risk işleme stratejileri etkisiz hale gelmiş olabilir. Bu durumda farklı bir risk işleme prosedürü geliştirmek gerekebilir. Öte yandan ilgili risk, kendisine tahsis edilen kaynakların geri yönlendirilmesine imkân verecek şekilde azalmış da olabilir.

Kurum ve kuruluşlarda risk yönetiminin başarıya ulaşması için, ilgili yönetim prosedür ve araçlarının tanımlanıp, uygulanmasının kurum kültürü haline getirilmesi gerekmektedir. Risk yönetim süreci bir döngü teşkil ettiğinden, belli periyotlarda bu döngüyü tekrar uygulamaya koyup, risklerin mevcut durumlarını ve yeni ortaya çıkan riskleri kuruluşların menfaatine olacak şekilde yönetmek önem arz etmektedir. Ancak

her döngüde tekrar aynı detaylı risk tanımlama ve işleme süreçleriyle karşı karşıya kalmamak için, kuruluşların risklerle ilgili olayları, önleme ve kontrol prosedürlerini, bu prosedürlerin sonuçlarını ve bunlarla ilgili tüm kayıtları tutarlı bir şekilde izleme ve değerlendirme yoluyla; tecrübe kazanması, bilgi toplaması ve kazanımlarını kayıt altına alması gerekir. Bu sebeple risk yönetimi sürecinin her aşaması uygun şekilde kaydedilmeli ve risklerle ilgili karar alma sürecindeki varsayımlar, yöntemler, veri kaynakları, sonuçlar ve nedenler kayıtlara düzenli bir şekilde eklenmelidir. Bu şekilde kuruluşlar, bu süreçlerle ilgili gelecekte karşılaşabilecekleri yasal, düzenleyici ve operasyonel ihtiyaçlarını karşılayabilecek ve aynı kayıtları tekrar oluşturmanın maliyetinden kaçınacaktır.

Örneğin, Amerika Birleşik Devletleri'nde risk değerlendirme süreci genellikle, Yönetim ve Bütçe Dairesi'nin A-130 sayılı ve Federal Bilgi Kaynaklarının Yönetimi başlıklı Genelgesi gereği, federal kuruluşlar tarafından asgari her üç yılda bir tekrarlanır. Ancak bilişim sistemleri için risk yönetimi, kanun veya yönetmelikle düzenlenmesinin ötesinde, kurum ve kuruluşun iş hedeflerini ve misyonunu destekleyen iyi bir uygulama olması sebebiyle tercih edilmeli ve özenli bir şekilde uygulanmalıdır. Kuruluşun risklerinin değerlendirilmesi ve işlenmesi için, özel bir yönetim programı oluşturulmalı ve bu program periyodik olarak süreç değişikliklerine izin verecek kadar esnek olmalıdır (Rosado, 2012).

Risk yönetiminin ve risk izlemenin rekabetçi bir iş ortamında hata ve arızalara hızlı bir şekilde cevap verebilmesi için, etkin ve doğru zamanlı bir gözden geçirme kritik önem taşımaktadır. Güncel bilgiler temin edebilecek çevikliklerinin olmaması sebebiyle, bulut tabanlı uygulamalardaki modern güvenlik tehditlerini tespit etmek için, geleneksel yöntemlere dayanan değerlendirme ve denetlenme modelleri artık geçerliliğini yitirmiştir.

Uygulamaların çalışma süresi verileri, arızaların kullanıcı tarafından düzeltilmesi ve riske hızla tepki verilmesi için gereklidir. Ancak çoğu sistem bilgisi, uygulamanın yanlış veya eski bir sunumunu vererek, ya yararlı olamayacak kadar geç ulaşır veya çok

kısıtlayıcı veya sınırlı bir kapsam sağlar. Bu sebeple, kullanıcıların gerçek zamanlı olarak, hızlı ve iyi bilgilendirilmiş kararlar almalarını sağlayan yeni bir web teknolojisi gereklidir. Bu teknolojinin, günümüzde uygulama çalışma süresinin değerlendirilmesi için gerekli ve en kritik üç faktör olan olaylar, log kayıtları ve izleme kayıtlarının hepsinin aynı anda kullanıldığı bir denetim modeli olması, herhangi bir bulut bilişim tabanlı sistemdeki tüm uygulamaların güvenliğinin ve dolayısıyla kalitesinin artması açısından çok önemlidir (Rosado, 2012).

4.6. Bulut Bilişim Risklerinin Profilleri

Bulut bilişim mimarisi ile ilgili kamu kurum ve kuruluşları ele alınarak gerçekleştirilen bu risk yönetimi çalışmasında; öncelikle mimariyi oluşturan varlıklar, bu varlıkları etkileme potansiyeline sahip tehditler ve zafiyetler ile birlikte, ilgili tehdit ve zafiyetlerin sebep olabileceği riskler belirlenmişti. Ardından bu risklerin kuruluşlar açısından kritikliğini ve önemini belirlemek amacıyla, risk olasılıkları ve risk etkileri değerlendirilmiş ve bu ikisiyle doğru orantılı bir kavram olan risk değerleri hesaplanmıştı. Son olarak, risk değerleri ve bu değerlere göre atanan risk dereceleri doğrultusunda, sıralanan ilgili risklere risk işleme yöntemleri uygulanmış ve bu kapsamda; her bir riske ne gibi risk azaltıcı kontrol ve önlemlerin uygulanabileceği, hangi risklerin ne şekilde başka kuruluşlara transfer edilebileceği, hangi risklerden ne şekilde kaçınılabileceği ve hangi risklerin kurum ve kuruluşlarca gerekli önlem ve kontrolleri uygulama ve düzenli izleme şartıyla kabul edilebilecek nitelikte olduğu gibi sorulara cevaplar aranmıştı. Bu kısımda, ilgili açıklamalarıyla gerçekleştirilen bu çalışmalar, her bir risk kalemi için özet olarak tek bir tabloda toplanacak ve ilgili riskin profili çıkarılacaktır. Bu sayede, periyodik olarak uygulanması gereken risk analizi ve yönetimi döngüsünün bir sonraki seferinde, ilgili riskin daha kolay bir şekilde incelenebilmesi için gerekli altyapı ve kısayollar sağlanmaya çalışılacaktır. Bu doğrultuda, aşağıdaki risk profili tablolarında her bir risk için; etkilenen varlıklara, tehdit ve zafiyetlere, risk olasılığına, risk etkisine, risk derecesine ve risk işleme yöntemlerine yer verilmiştir:

Riskin Adı	Yönetim ve Kontrol Kaybı							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.7- Bulut Harici Sözleşme Kaynaklı Sorumluluklar T.8- Belgelendirme Programlarının Bulut Altyapısına Adapte Olmaması Z.9- Standart Teknoloji Ve Çözümlerin Eksikliği Z.10- Kaynak Emanet Anlaşması Eksikliği Z.12- Güvenlik Açığı Değerlendirme Sürecinin Bulunmaması Z.15- Gizli Bağımlılık Yaratan Alt Yükleniciler Z.16- Farklı Paydaşlara Verilen Sözlerle Çelişen Hizmet Seviye Anlaşması Hükümleri Z.18- Müşterilere Denetim ve Belgelendirme Yetkisi Verilmemesi Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.26- Belirsiz Görev ve Sorumluluklar Z.27- Zayıf Rol Tanımı Uygulamaları Z.33- Varlık Mülkiyeti Belirsizliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Beklenen							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.2: R.1-Yönetim ve Kontrol Kaybı Risk Profili

Riskin Adı	Bulut Hizmeti Sonlandırması veya Arızası							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.11- Kötü Sağlayıcı Seçimi Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Çok Düşük Olasılık							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.3: R.2- Bulut Hizmeti Sonlandırması veya Arızası Risk Profili

Riskin Adı	Servis Sağlayıcı Bağımlılığı							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.20- Müşteri hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.11- Kötü Sağlayıcı Seçimi Z.9- Standart Teknoloji Ve Çözümlerin Eksikliği Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Büyük İhtimalle							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.4: R.3- Servis Sağlayıcı Bağımlılığı Risk Profili

Riskin Adı	Üçüncü Parti Tedarikçi Hatası							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.11- Kötü Sağlayıcı Seçimi Z.15- Gizli Bağımlılık Yaratan Alt Yükleniciler Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Çok Düşük Olasılık							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.5: R.4- Üçüncü Parti Tedarikçi Hatası Risk Profili

Riskin Adı	Bulut Sağlayıcı Kuruluşun Satın Alınması							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.6: R.5- Bulut Sağlayıcı Kuruluşun Satın Alınması Risk Profili

Riskin Adı	Uyum Sorunları							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.23- Belgelendirme							
İlgili Tehdit ve Zafiyetler	T.8- Belgelendirme Programlarının Bulut Altyapısına Adapte Olmaması Z.9- Standart Teknoloji Ve Çözümlerin Eksikliği Z.18- Müşterilere Denetim ve Belgelendirme Yetkisi Verilmemesi Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Beklenen							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.7: R.6- Uyum Sorunları Risk Profili

Riskin Adı	Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı							
Risk Sınıfı	Kurumsal ve Stratejik Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.20- Müşteri hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.1- Hipervizörle İlgili Tehditler T.2- Kaynak İzolasyon Eksikliği Z.5- İtibar Ayrımı Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	X

Tablo 4.8: R.7- Sağlayıcının Diğer Müşterileri Nedeniyle İtibar Kaybı Risk Profili

Riskin Adı	Dış Kaynaklı Saldırılar							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.8- Bulut hizmeti yönetim arabirimi V.14- Ağ ve haberleşme yazılımları V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.24- İş taahhütleri							
İlgili Tehdit ve Zafiyetler	T.12- Yanlış Yapılandırma T.13- Sistem veya İşletim Sistemi Tehditleri Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.3- Yeniden Yapılandırma Zafiyetleri Z.4- Yönetim Arayüzüne Uzaktan Erişim Z.20- Kaynak Üst Limitleri ile İlgili Politika Belirlenmemesi Z.39- Yetersiz Filtreleme Kaynakları							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.9: R.8- Dış Kaynaklı Saldırılar Risk Profili

Riskin Adı	Verilerin Güvensiz veya Etkisiz Silinmesi							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.4- Kimlik bilgileri							
İlgili Tehdit ve Zafiyetler	Z.14- Veri Silme ve Ortam Temizlemesi							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Olası							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.10: R.9- Verilerin Güvensiz veya Etkisiz Silinmesi Risk Profili

Riskin Adı	Nakil Halindeki Veriyi Yakalama							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.7- Yedekleme ve arşiv verileri V.17- Kuruluş itibari V.18- Müşteri güveni V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	T.5- İç Ağda Tarama İşlemi T.6- Müşterek İkamet Taramaları T.3- İletişim Şifreleme Tehditleri Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.6- Aktarılan Veri veya Arşivde Şifreleme Eksikliği Veya Zayıflığı Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.11: R.10- Nakil Halindeki Veriyi Yakalama Risk Profili

Riskin Adı	Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	T.13- Sistem veya İşletim Sistemi Tehditleri Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.7- Veriyi Şifrelenmiş Biçimde İşlemenin Olanaksızlığı Z.26- Belirsiz Görev ve Sorumluluklar Z.27- Zayıf Rol Tanımı Uygulamaları Z.28- Gereksiz Yetkiler Verilmesi Z.29- Yetersiz Fiziksel Güvenlik Prosedürleri Z.36- Kötü Yama Yönetimi ve Uygulama Açıkları							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Olası							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.12: R.11- Bulut Sağlayıcı Tarafında Kötü Amaçlı Giriş Risk Profili

Riskin Adı	Kaynak Tükenmesi							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.11- Erişim kontrol, doğrulama ve yetkilendirme yazılımları V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	Z.11- Kaynak Kullanımının Yanlış Modellenmesi Z.19- Yetersiz Kaynak Sağlama ve Altyapı Yatırımları Z.20- Kaynak Üst Limitleri ile İlgili Politika Belirlenmemesi Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.13: R.12- Kaynak Tükenmesi Risk Profili

Riskin Adı	Şifreleme							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.13- Müşteri uygulamaları V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.24- İş taahhütleri							
İlgili Tehdit ve Zafiyetler	T.3- İletişim Şifreleme Tehditleri T.4- Anahtar Oluşturma Tehditleri Z.6- Aktarılan Veri veya Arşivde Şifreleme Eksikliği Veya Zayıflığı Z.7- Veriyi Şifrelenmiş Biçimde İşlemenin Olanaksızlığı Z.8- Zayıf Anahtar Yönetimi Z.9- Standart Teknoloji Ve Çözümlerin Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Büyük İhtimalle							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.14: R.13- Şifreleme Risk Profili

Riskin Adı	Kaynak İzolasyonu Eksikliği							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.1- Hipervizörle İlgili Tehditler T.2- Kaynak İzolasyon Eksikliği T.5- İç Ağda Tarama İşlemi T.6- Müşterek İkamet Taramaları Z.5- İtibar Ayrımı Eksikliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Olası							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.15: R.14- Kaynak İzolasyonu Eksikliği Risk Profili

Riskin Adı	Hizmet Kesintisi veya Bozulması							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.8- Bulut hizmeti yönetim arabirimi V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.12- Yanlış Yapılandırma T.13- Sistem veya İşletim Sistemi Tehditleri Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.36- Kötü Yama Yönetimi ve Uygulama Açıkları							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.16: R.15- Hizmet Kesintisi veya Bozulması Risk Profili

Riskin Adı	Kötü Amaçlı Araştırma veya Taramalara Girişilmesi							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.5- İç Ağda Tarama İşlemi T.6- Müşterek İkamet Taramaları							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.17: R.16- Kötü Amaçlı Araştırma veya Taramalara Girişilmesi Risk Profili

Riskin Adı	Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	Z.16- Farklı Paydaşlara Verilen Sözlerle Çelişen Hizmet Seviye Anlaşması Hükümleri Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.26- Belirsiz Görev ve Sorumluluklar							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.18: R.17- Müşteri Gereksinimleri ve Bulut Ortamı Arasındaki Uzlaşmazlık Risk Profili

Riskin Adı	Şifreleme Anahtarlarının Kaybı							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.4- Kimlik bilgileri V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	T.4- Anahtar Oluşturma Tehditleri Z.8- Zayıf Anahtar Yönetimi							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.19: R.18- Şifreleme Anahtarlarının Kaybı Risk Profili

Riskin Adı	Hizmet Motorunun Hacklenmesi							
Risk Sınıfı	Teknik Riskler ve Güvenlik Riskleri							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.1- Hipervizörle İlgili Tehditler T.2- Kaynak İzolasyon Eksikliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.20: R.19- Hizmet Motorunun Hacklenmesi Risk Profili

Riskin Adı	Yargı Değişiminden Kaynaklanan Riskler							
Risk Sınıfı	Hukuksal Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Beklenen							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.21: R.20- Yargı Değişiminden Kaynaklanan Riskler Risk Profili

Riskin Adı	Mahkeme Celbi ve E-Keşif							
Risk Sınıfı	Hukuksal Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.2- Kaynak İzolasyon Eksikliği Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Büyük İhtimalle							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.22: R.21- Mahkeme Celbi ve E-Keşif Risk Profili

Riskin Adı	Veri Sansürü							
Risk Sınıfı	Hukuksal Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	T.7- Bulut Harici Sözleşme Kaynaklı Sorumluluklar T.11- Kötü Sağlayıcı Seçimi Z.17- Aşırı İş Riski İçeren Hizmet Seviye Anlaşması Hükümleri Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.33- Varlık Mülkiyeti Belirsizliği Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.23: R.22- Veri Sansürü Risk Profili

Riskin Adı	Lisans Riskleri							
Risk Sınıfı	Hukuksal Riskler							
Etkilenen Varlıklar	V.17- Kuruluş itibari V.20- Müşteri hizmet sunumu V.23- Belgelendirme							
İlgili Tehdit ve Zafiyetler	Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	X

Tablo 4.24: R.23- Lisans Riskleri Risk Profili

Riskin Adı	Veri Koruma Riskleri							
Risk Sınıfı	Hukuksal Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	Z.21- Birden Fazla Yargıya Tabi Farklı Bölgelerde Veri Depolama ve Şeffaflık Eksikliği Z.22- Yargı Mevzuatı Hakkında Bilgi Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Büyük İhtimalle							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	X

Tablo 4.25: R.24- Veri Koruma Riskleri Risk Profili

Riskin Adı	Ayrıcalık Yükseltme Olasılığı							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.6- Kullanıcı dizini V.11- Erişim kontrol, doğrulama ve yetkilendirme yazılımları							
İlgili Tehdit ve Zafiyetler	T.1- Hipervizörle İlgili Tehditler T.12- Yanlış Yapılandırma Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.3- Yeniden Yapılandırma Zafiyetleri Z.26- Belirsiz Görev ve Sorumluluklar Z.27- Zayıf Rol Tanımı Uygulamaları Z.28- Gereksiz Yetkiler Verilmesi							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.26: R.25- Ayrıcalık Yükseltme Olasılığı Risk Profili

Riskin Adı	İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.7- Yedekleme ve arşiv verileri V.15- Fiziksel donanım (istemci, sunucu, depolama ünitesi, ağ ve haberleşme donanımı vb.) V.17- Kuruluş itibari V.18- Müşteri güveni							
İlgili Tehdit ve Zafiyetler	Z.29- Yetersiz Fiziksel Güvenlik Prosedürleri							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Çok Düşük Olasılık							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.27: R.26- İzinsiz Fiziksel Erişim ve Bilişim Ekipmanının Çalınması Risk Profili

Riskin Adı	Ağ Kesilmeleri							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.15- Fiziksel donanım (istemci, sunucu, depolama ünitesi, ağ ve haberleşme donanımı vb.) V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	T.2- Kaynak İzolasyon Eksikliği T.12- Yanlış Yapılandırma T.13- Sistem veya İşletim Sistemi Tehditleri Z.30- Yetersiz İş Sürekliliği ve Felaket Kurtarma Planı veya Eksikliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.28: R.27- Ağ Kesilmeleri Risk Profili

Riskin Adı	Sosyal Mühendislik Saldırıları							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.4- Kimlik bilgileri V.11- Erişim kontrol, doğrulama ve yetkilendirme yazılımları V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.22- Fikri mülkiyet hakları							
İlgili Tehdit ve Zafiyetler	T.2- Kaynak İzolasyon Eksikliği T.3- İletişim Şifreleme Tehditleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.24- Güvenlik Gereksinimleri Farkındalık Eksikliği Z.29- Yetersiz Fiziksel Güvenlik Prosedürleri							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer		Kaçınma	

Tablo 4.29: R.28- Sosyal Mühendislik Saldırıları Risk Profili

Riskin Adı	Hizmet Ücreti Değişikliği							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.24- İş taahhütleri							
İlgili Tehdit ve Zafiyetler	T.7- Bulut Harici Sözleşme Kaynaklı Sorumluluklar T.11- Kötü Sağlayıcı Seçimi Z.17- Aşırı İş Riski İçeren Hizmet Seviye Anlaşması Hükümleri Z.23- Kullanım Şartlarında Bütünlük ve Şeffaflık Eksikliği Z.35- Sağlayıcı Yedeklilik Eksikliği							
Risk Etkisi	Hafif Etki							
Risk Olasılığı	Olası							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.30: R.29- Hizmet Ücreti Değişikliği Risk Profili

Riskin Adı	Ağ Trafiğini Değiştirme							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.24- İş taahhütleri							
İlgili Tehdit ve Zafiyetler	T.3- İletişim Şifreleme Tehditleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.3- Yeniden Yapılandırma Zafiyetleri Z.12- Güvenlik Açığı Değerlendirme Sürecinin Bulunmaması							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.31: R.30- Ağ Trafiğini Değiştirme Risk Profili

Riskin Adı	Yedeklerin Kaybolması veya Çalınması							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.7- Yedekleme ve arşiv verileri V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.3- Yeniden Yapılandırma Zafiyetleri Z.29- Yetersiz Fiziksel Güvenlik Prosedürleri							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	ORTA							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.32: R.31- Yedeklerin Kaybolması veya Çalınması Risk Profili

Riskin Adı	Doğal Afetler							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.1- Kişisel veriler V.2- Kişisel hassas veriler V.3- İnsan kaynağı verileri V.7- Yedekleme ve arşiv verileri V.17- Kuruluş itibari V.18- Müşteri güveni V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu							
İlgili Tehdit ve Zafiyetler	Z.30- Yetersiz İş Sürekliliği ve Felaket Kurtarma Planı veya Eksikliği							
Risk Etkisi	Şiddetli Etki							
Risk Olasılığı	Çok Düşük Olasılık							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.33: R.32- Doğal Afetler Risk Profili

Riskin Adı	Ağ Yönetimi Sorunları							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.14- Ağ ve haberleşme yazılımları V.17- Kuruluş itibari V.18- Müşteri güveni V.19- Çalışan sadakati ve deneyimi V.20- Müşteri hizmet sunumu V.21- Sağlayıcı hizmet sunumu V.24- İş taahhütleri							
İlgili Tehdit ve Zafiyetler	T.2- Kaynak İzolasyon Eksikliği T.12- Yanlış Yapılandırma T.13- Sistem veya İşletim Sistemi Tehditleri Z.30- Yetersiz İş Sürekliliği ve Felaket Kurtarma Planı veya Eksikliği							
Risk Etkisi	Yıkıcı Etki							
Risk Olasılığı	Olası							
Risk Değeri	YÜKSEK							
Risk İşleme Yöntemi	Kabul Etme		Azaltma	X	Transfer	X	Kaçınma	

Tablo 4.34: R.33- Ağ Yönetimi Sorunları Risk Profili

Riskin Adı	Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması							
Risk Sınıfı	Buluta Özgü Olmayan Diğer Riskler							
Etkilenen Varlıklar	V.5- Operayonel ve güvenlik logları							
İlgili Tehdit ve Zafiyetler	T.13- Sistem veya İşletim Sistemi Tehditleri Z.1- Kimlik Doğrulama, Yetkilendirme ve Kullanıcı Hesabı Zafiyetleri Z.2- Kullanıcı Yapılandırma Zafiyetleri Z.3- Yeniden Yapılandırma Zafiyetleri Z.13- Adli Mevzuat Eksikliği Z.38- Log Kayıtları İle İlgili Politika Ve Prosedürlerinin Eksikliği							
Risk Etkisi	Ciddi Etki							
Risk Olasılığı	Az Olası							
Risk Değeri	DÜŞÜK							
Risk İşleme Yöntemi	Kabul Etme	X	Azaltma	X	Transfer		Kaçınma	

Tablo 4.35: R.34- Operasyonel ve Güvenlik Log Kayıtlarının Kaybolması veya Bozulması Risk Profili

SONUÇ

Geride bıraktığımız yüzyılda her alanda yaşanan teknolojik gelişmeler, 1950'li yıllarda bilgisayarların ve buna paralel olarak bilişim teknolojilerinin hayatımıza girmesini sağlamış ve özellikle son otuz yılda baş döndürücü bir şekilde gelişen bilişim teknolojileri insanoğlunun sosyal yaşamını belirleyici bir rol kazanmıştır. Bugün eğitim, sağlık, ulaşım, perakende, finans, güvenlik, iletişim, eğlence, bilgi edinme gibi hayatın her alanında etkin şekilde kullanılan internet teknolojileri yoluyla; kullanıcıların birçok işlemi mekan ve platform bağımsız olarak gerçekleştirmesi rutin hale gelmiştir. Bulut bilişim mimarileri de, yaşanan hızlı ve talep odaklı değişim ve gelişimlerin, bilişim teknolojilerini halihazırda getirdiği son nokta olarak değerlendirilebilir. Platform bağımsız yaygın ağ erişimi, esneklik, ölçülebilirlik, talep üzerine self servis ve kaynak havuzu oluşturma gibi birçok kabiliyeti bünyesinde barındıran bulut bilişimi, yeni bir bilişim teknolojisi olarak tanımlamaktansa; sanallaştırma, çoklu kiracılık, servis odaklı mimari, istemci-sunucu modeli, API, dağıtımlı hesaplama ve Web 2.0 gibi öncül kavram ve teknolojilerle etkileşim içerisinde kullanıcılara daha düşük maliyetle, daha yüksek performans ve kalitede hizmet sunabilen bir hizmet modeli olarak değerlendirmek daha doğru olacaktır.

Servis olarak Yazılım, Servis olarak Platform, Servis olarak Altyapı vb. servis modelleri sunan bulut bilişim mimarilerinde, kullanıcıların hizmet ihtiyaçlarının çeşidini ve bu ihtiyaçları karşılayacak kaynakları belirlemeleri yeterli olmakta, kaynak miktarı talep doğrultusunda istenildiği zaman ayarlanabilmektedir. Açık bulut, özel bulut, hibrit bulut ve topluluk bulutu gibi mimarilere sahip bulut bilişimde, ilgili müşteri kuruluşun mimari seçimi, sunulan uygulama ve verinin gizlilik derecesine ve yürütülen hizmetin niteliğine göre şekillenmektedir. Örneğin, bir kuruluşun sadece kendi iç operasyonları veya veri mahremiyeti içeren uygulamaları için, kendi özel bulut mimarisini kurması uygun olacakken; veri mahremiyeti ile ilgili herhangi bir kısıtlaması olmayan ve uygulamalarını tüm vatandaşlara sunan kuruluşların, açık bulut mimarilerini kullanmaları daha doğru olacaktır. Her iki tipte hizmetler sunan kuruluşlar içinse, hibrit

bulut mimarisi tavsiye edilmektedir. Bu doğrultuda, çoğu kamu kuruluşu için hibrit bulut mimarisinin tercihi ön plana çıkacaktır.

Sağladığı sayısız avantajın yanında bulut bilişim; ağ ve bant genişliği, veri gizliliği ve güvenliği, mevzuat, yargı ve denetim, güvenilirlik ve veri yönetimi ile hizmet seviye anlaşmaları vb. konularla ilgili çeşitli riskleri de barındırmaktadır. Müşteri kuruluşların ve bulut sağlayıcılarının bu risklerin farkında olması ve gerektiğinde riskleri önleyici veya bertaraf edici aksiyonlar alması önem arz etmektedir.

E-devlet politika, strateji ve çalışmalarının; internet ve sosyal medya üzerinden platform bağımsız şekilde sunulan, vatandaş odaklı ve vatandaşların yönetim süreçlerine dâhil olabildikleri c-devlet çalışma ve politikalarına dönüştüğü günümüzde; kamuda bulut bilişim kullanımı bir tercih değil zorunluluk haline gelmiştir. Kamu hizmetlerinin vatandaşlara kamu daireleri yerine internet üzerinden farklı lokasyon ve platformlarda sunulmasının, hem vatandaş ve hem de kamu kuruluşlarına sağladığı maliyet tasarruflarının yanında; vatandaşların sunulan hizmetlerle ilgili yaptıkları tercih ve belirttikleri görüşleriyle, merkezi ve yerel yönetime dolaylı da olsa katkıda bulunabilmeleri, demokrasinin gelişimi açısından kritik önem taşımaktadır. Örneğin e-referandum yoluyla vatandaşların yasal düzenlemeler konusunda karar verebilmesi, kamu idaresi tarafından yapılması öngörülen bir kısım hizmetler içerisinden önemli gördüklerini önceliklendirebilmesi veya yapılan bir hizmetin ismine ve niteliklerine karar verebilmesi bulut bilişim mimarileriyle giderek kolaylaşmaktadır.

Gelişmiş ve gelişmekte olan ülkelerin, bulut bilişimle ilgili uyguladıkları yedi kilit politikaya göre güçlü ve zayıf yönleri üzerinden değerlendirildiği 2016 BSA Global Bulut Bilişim Puan Çizelgesi adlı çalışmada ülkemiz 19. sırada gösterilmiştir. Bu durum ülkemizin açısından, kamusal alanda bulut bilişim mimarisinin kurulması, benimsenmesi ve kullanımı için atılması gereken birçok adım bulunduğu anlamını taşımaktadır. Bunlardan ilki kuruluşların kendi bulut altyapılarını kurmaları veya bir hizmet sağlayıcı seçerek ilgili bilişim ihtiyaçlarını kiralamaları ile ilgili karar sürecidir. Maliyet tasarrufu açısından, kuruluşların kendi bulut altyapılarını kurmaları ve işletmeleri yerine, mümkün

olduğunca bilişim kaynağı kiralama yoluna gitmeleri mantıklı olacaktır. Bu noktada bulut hizmet sağlayıcısı seçimi kritik rol oynamaktadır. Dünyadaki örneklere bakıldığında, bulut bilişim sağlayıcıları piyasadaki özel sektör kuruluşları arasından olabileceği gibi, bu konuda görevlendirilmiş bir kamu ajansı/kurum veya yine devletin ilgili organları tarafından görevlendirilmiş Bilgi İletişim Teknolojileri (BİT) sağlayıcısı da olabilmektedir. Yine bulut bilişim alanında yeterli tecrübesi bulunmayan kuruluşların, ilgili hizmeti temin etmek için bulut aracıları (broker) kullandığı birçok örnekler mevcuttur. Burada kritik nokta, bulut bilişimle ilgili veri gizliliği ve güvenliği, veri sahipliği, fikri mülkiyet hakları, denetim, uluslararası kurallara uyum, bulut bilişim alt yüklenicileri vb. alanlarda yasal düzenlemelerin yapılması gereksinimidir. İlgili mevzuatların oluşturulmasını müteakip, bu mevzuatları temel alacak şekilde bulut bilişimle ilgili ulusal standartların oluşturulması ve kamu kuruluşlarının sağlayıcılarla imzalayacağı ilgili hizmet seviye anlaşmalarında bu standartlara atıfta bulunularak, sağlayıcının standartlar doğrultusunda hizmet sunması temin edilmelidir. Bu doğrultuda Bulutu Bilişim Kullanım ve Güvenlik Standardı Taslağı 07.03.2014 tarihinde yayınlanmıştır. Bulut bilişimle ilgili mevzuatın belirlenmesi, kamu kuruluşlarına bu mimarilere geçiş sürecinde destek verilmesi ve gerekli altyapının sağlanması amaçlarıyla; ülke genelinde bu konudan sorumlu bir kurumun belirlenmesi kritik öneme sahiptir. Bu doğrultuda, ülkemizde kamu bulut bilişim altyapısının oluşturulması hedefinin Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından; TÜBİTAK, TÜRKSAT, TSE işbirliğiyle ve öncelikle veri merkezlerinin bütünleştirilmesinden başlanarak gerçekleştirilmesi planlanmaktadır. Bu sayede, kamu kurum ve kuruluşlarında strateji ve politikalar tek elden, diğer kamu kurumlarıyla koordineli bir biçimde belirlenecek ve mümkün olduğunca mükerrer ve birbiriyle uyumsuz sistem yatırımları engellenebilecektir.

Gelişmiş ülkelerin bazılarında, ilgili bulut hizmetinin kamu kuruluşları tarafından kolayca temin edilebilmesi için; belirli kriterleri sağlayan sağlayıcıların listeleri ve bu sağlayıcılarla yapılacak tip hizmet seviye anlaşmaları, bulut bilişim alanında sorumlu kuruluşlar tarafından sunulmaktadır. Herhangi bir bulut servisinden yararlanmak isteyen

kuruluşun, belirtilen listedeki sağlayıcıyla irtibata geçerek kendi sunacağı hizmetle ilgili ister ve şartlarını belirtmesi yeterli olmaktadır. Ülkemizde bulut bilişimle ilgili strateji ve politikaların belirlenmesi sürecinde, dünya ölçeğinde ilgili mevzuat ve standartların oluşturulması ile kamu bulutları ve entegre veri merkezleri kurulumu ve işletilmesi alanlarında başarı sağlamış ülkeler olan Japonya, ABD, Almanya, İngiltere ve Güney Kore gibi öncü ülkelerin bu konudaki faaliyetlerinin incelenmesi faydalı olacaktır. Yine bu çalışmanın ikinci bölümünün sonunda yer verilen, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA), Avrupa ülkelerinde bulut bilişimin benimsenmesine ilişkin Avrupa'daki mevcut duruma ve elde edilen senaryolara göre güvenli kamu bulutları kurulmasına yönelik ortaya koyduğu tavsiye ve çözüm önerileri dikkate alınmalıdır.

Diğer bir adım, kamu kurum ve kuruluşlarının kendi faaliyet alanları ve yasal gereksinimleri çerçevesinde; hangi bulut mimarilerini, ne şekilde ve hangi hizmetleri için kullanmaları gerektiğini belirlemeleridir. Ülkemizde geçerli mevzuat uyarınca, gizlilik derecesi olan veya hizmete özel kritik ve hassas evraklar ve vatandaşlara ait kişisel bilgilerin veri tabanlarında tutulduğu iş ve hizmetlerle ilgili, kuruluşların özel bulut mimarilerini kullanmaları gerekecektir. Ancak, veri gizliliği içermeyen ve çalınması, kaybolması veya ifşa edilmesi kuruluşlara sorumluluk yüklemeyecek veri ve bu verileri kullanan uygulamaların açık bulut mimarilerinde barındırılmasında bir sakınca bulunmamaktadır. Kamu kuruluşlarının birçoğunda her iki tür veri ve bu verileri kullanan uygulamalar bulunabileceği için, açık ve özel bulut mimarilerinin bileşimi olan hibrit bulut mimarisinin kullanılması en doğru seçenek olacaktır. Yine benzer sektörlerde faaliyet gösteren kamu kuruluşlarının benzer gereksinimlerine göre düzenlenebilecek ve gerektiğinde değişen ihtiyaçlara göre özelleştirilebilecek topluluk bulutu mimarilerinin kullanımı uygun bir seçenektir.

Bulut bilişime aktarım sürecinde yaşanacak zorluklara çözümler aranması diğer bir kritik adım olarak ön plana çıkmaktadır. Bu noktada, kamu kurum ve kuruluşlarının bulut bilişim mimarilerine hangi uygulama ve servislerini aktarıp aktaramayacaklarını belirlemeleri ve eğer gerekiyorsa bazı uygulamalarının bulut mimarisinde çalışabilmesi

için gerekli revizyonları yapmaları gerekmektedir. Bu süreçte, geleneksel istemci-sunucu mimarisinde yazılan uygulamaların bulut mimarisine aktarılabilmesi için neredeyse yeniden yazılması gerebilecekken, dağıtık mimarilerde yazılmış uygulamalar az bir çabayla aktarılabilecektir. Kuruluşların bu sebeple, aktarım sürecini dikkatlice planlanmaları ve özellikle e-devlet üzerinden sunacakları uygulamaların aktarımında belli bir yol haritası belirlemeleri gereklidir. Bu doğrultuda, kamu kurum ve kuruluşlarının takip edebileceği; strateji tanımlama, mevcut mimariyi belirleme ve anlama, buluta aktarım planı hazırlama, sağlayıcı seçimi, analiz ve test, haritalama ve aktarma ve yönetim adımlarına, çalışmanın ikinci bölümünde yer verilmiştir. Ayrıca kamu kurum ve kuruluşlarınca temin edilecek yeni uygulama yazılımlarının, bulut mimarisine uygun şekilde tasarlanması stratejisinin belirlenmesi gerekmektedir. Bu sayede, orta vadede atıl duruma düşecek yazılımlar için kaynak tahsis edilmesinin önüne geçilebilecektir.

Bulut bilişimin ülke sathında yaygınlaştırılabilmesi için gerekli diğer bir husus, kısa vadede oluşacak uygulama yazılımı ihtiyacının mümkün olduğunca yerli ve milli yazılım firmalarınca karşılanabilmesi için gerekli destek ve teşviklerin sağlanmasıdır. Bu sebeple, gerekli Ar-Ge yatırımlarının kamu, üniversite ve özel sektör işbirliğiyle yapılması, bulut bilişim mimarileri ile ilgili yetkin personelin yetiştirilmesi için gerekli eğitimlerin verilmesi ve yazılımlarla ilgili gerekli teknik, yasal ve organizasyonel standartların yayımlanması gereklidir.

Bulut bilişimin kamusal ölçekte kullanılması ve yaygınlaştırılması için diğer bir adım, kurulacak kamu bulutları vasıtasıyla kamu kuruluşlarının işbirliğini ve birlikte çalışabilirliğini arttırmak için gerekli koordinasyonun sağlanmasıdır. Aynı tip hizmeti sunan kuruluşların mükerrer yatırımlar yapmaması için, ilgili hizmet alanlarında üst kuruluşlar belirlenerek, ilgili kamu bulutunun kurulması sorumluğu bu kuruluşlara aktarılabilir. Örnek olarak, coğrafi veri servisleri için oluşturulabilecek bir coğrafi veri bulutunun Çevre ve Şehircilik Bakanlığı koordinasyonunda kurulup, oluşturulan şablon kent bilgi sistemi, e-imar vb. uygulamaların; bu konular için yatırım bütçesi temin edemeyen küçük ölçekli yerel yönetimlere servis edilerek, kendi uygulamalarını

geliştirme imkânı tanınması verilebilecektir. Yine diğer kamu kuruluşlarının harita tabanlı uygulamalarına bu bulut üzerinde tutulan coğrafi verilerin altlık olarak sunulması sağlanabilecektir.

Bulut bilişim, kamu kuruluşlarının kullanımı ile ilgili sağlayacağı fayda ve avantajların yanında; birçok zafiyet, tehdit ve bunlara bağlı olarak ortaya çıkan riskler de içermektedir. Bu riskler bulut bilişime özgü riskler olabilecekleri gibi, geleneksel bilişim mimarilerinde görülen riskler de olabileceklerdir. Hizmet devamlılığı ve kullanılabilirliği, hizmet sağlayıcı bağımlılığı, veri güvenliği ve gizliliği, veri denetlenebilirliği, uygunluğu ve yasal düzenlemeler, ağ ve bant genişliği, yönetim ara yüzü, veri transferi, sağlayıcı alt yüklenicileri ve lisanslama vb. ana başlıklarda toplanabilecek toplam 34 adet risk unsuru, bu çalışmada irdelenmiş ve bu risklerin etki ve olasılıklarının azaltılabilmesi için TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27005 Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Risk Yönetimi ve TS ISO 31000 Risk Yönetimi Standartları çerçevesinde gerekli risk işleme prosedürleri uygulanmıştır. Bu kapsamda ilk etapta kuruluşun risklerden etkilenebilecek varlıkları belirlenmiştir. Bu varlıklar üzerindeki herhangi bir tehdit ve zafiyet, ilgili kuruluş için bir risk unsurudur. Bu doğrultuda, varlıkların belirlenmesini müteakiben, bu varlıklarla ilgili ortaya çıkabilecek tehdit ve zafiyetler ve hemen ardından bu tehdit ve zafiyetler sebebiyle oluşabilecek riskler ortaya konulmuştur. Bu çalışmada önemli görülen toplam 53 adet tehdit ve zafiyet incelenmiştir. Bu tehdit ve zafiyetlerin her biri, kuruluşun birden fazla riskine etki edebileceği gibi, bir risk birden fazla tehdit ve zafiyete bağlı olarak da oluşabilecektir. Bu sebeple çalışmanın son bölümünde, her bir risk unsuru ile ilgili risk profili oluşturularak; hangi riskin hangi varlıklar üzerinde etkili olduğu ve hangi tehdit veya zafiyetler sebebiyle oluştuğuna ilişkin eşleştirmeler yapılmıştır.

Risklerin belirlenmesinin ardından, bu risklerin kamu kurum ve kuruluşları için ne derece kritik olduklarını belirlemek amacıyla, risk değeri ve risk derecesi bulma prosedürü uygulanmıştır. İlgili risk değerlerinin ve buna bağlı risk derecelerinin hesaplanabilmesi için, risklerin etki değerleri ve meydana gelme olasılıkları

bulunmuştur. Bulunan risk olasılık ve etki değeri bileşenlerinin bir fonksiyonu olan risk değerleri hesaplanmış ve bu değerlere göre risk derecelendirme matrisi oluşturularak ve riskler sahip oldukları risk değerlerine göre kategorize edilerek; yüksek, orta ve düşük olmak üzere üç adet risk derecesi belirlenmiştir.

Son bölümde ilgili riskler, risk değerlerine ve risk derecelerine göre küçükten büyüğe sıralanmış ve sırasıyla risk işleme prosedürlerine tabi tutulmuşlardır. Bu prosedürlerin yöntemlerinden biri olan risk kabul etme, literatürde düşük dereceli risklere uygulanan bir risk işleme yöntemidir. Bu doğrultuda, düşük dereceli olarak belirlenen riskler için gerekli risk azaltıcı önlem ve kontroller belirlenmiş ve bunlarla birlikte periyodik olarak risk izleme ve değerlendirme prosedürlerinin uygulanması yoluyla, düşük dereceli risklerin kabul edilebileceği sonucuna varılmıştır. Orta ve yüksek dereceli riskler içinse, öncelikle yine risk azaltıcı önlem ve kontroller belirlenmiş ve bunların uygulanması halinde dahi, riskin hala ilgili faaliyet için kabul edilemeyecek seviyelerde olması durumu için; eğer uygulanması mümkünse diğer risk işleme yöntemleri olan risk transferi ve riskten kaçınma yolları incelenmiştir. Risk işleme prosedürünün uygulanmasının ardından diğer bir önemli konu, risklerle ilgili uygulanacak önlem ve kontrollerin fayda maliyet analizidir. İlgili kontrollerin, kuruluşlar için verimli şekilde uygulanabilmesi için gerekli yol haritası ve kriterler açıklanmıştır.

Risk yönetimi süreci, kuruluşlar için bir döngü şeklinde uygulanmalıdır. Kuruluşlar sahip oldukları riskleri, o risklerden etkilenecek varlık sahibi birimin öncülüğünde, riskin derecesine ve kritikliğine göre her bir risk için ayrı belirlenecek periyotlarda değerlendirmeli ve risk yönetimi döngüsünü en baştan uygulamalıdır. Bunun sebebi, ilgili riskin olasılık ve etki değerinin kuruluşun değişen faaliyetlerine göre değişim gösterebilmesi ve düşük risk seviyesine sahip bir riskin daha yüksek bir risk derecesine geçiş yapabilmesidir. Bunun yanında ilgili riskin değeri, uygulanan kontrolleri gereksiz hale getirecek şekilde azalmış olabilir veya etki alanı değişebilir. Ayrıca kuruluşun değişen faaliyetleri sebebiyle yeni riskler de ortaya çıkabilir. Bu

sebeple, kuruluşların belirledikleri risklerin takibi için kapsamlı bir risk izleme süreci belirlemeleri ve belli periyotlarda risk yönetim sürecini tekrarlamaları gerekmektedir.

Bu çalışma, günümüzde birçok kamu kurum ve kuruluşunun ilgi odağı haline gelen bulut bilişim ile ilgili olarak; karşılaşılabilecek riskleri belirleyen, analiz eden ve değerlendiren bir risk yönetimi modeli ihtiyacına cevap vermek amacıyla yapılmıştır. Bu alanda Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), Bulut Güvenliği Ajansı (CSA), Microsoft, ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) vb. kuruluşların, bulut bilişim mimarilerinde karşılaşılabilecek riskleri belirleme ve derecelendirme üzerine çalışmaları bulunmaktadır. Ancak bu çalışmalarda, belirlenen riskleri bertaraf etmek veya azaltmak için alınacak tedbirler, uygulanacak kontroller ve risk yönetimi döngüsündeki diğer birçok süreçten bahsedilmemiştir. Bu anlamda bu çalışma, kamu kuruluşları ve yine bulut bilişim mimarilerinden faydalanmak isteyen özel sektör kuruluşları için, bir çerçeve çizmek ve bir risk yönetim modeli ortaya koymak suretiyle, alanına katkıda bulunmaktadır. Burada belirtilen başlıca riskler, bu risklere etki eden tehdit ve zafiyetler ile risklerden etkilenen varlıklar; kuruluşlara göre farklılık gösterebilir. Yine her kuruluşta ilgili riskin olasılığı, etki değeri ve dolayısıyla risk değeri ve derecesi de değişebilir. Bu sebeple, her kuruluşun organizasyon yapısını ve faaliyet alanlarını dikkate alarak bu modeli uygulaması gerekecektir. Ancak yine de çoğu kamu ve özel sektör kuruluşu, bulut bilişim mimarilerinin etkin şekilde kurulması ve işletilmesi ile birlikte; ortaya çıkabilecek risklerin yönetilmesi hususlarında bu çalışmadan faydalanabilecektir.

Ris

k yönetim süreci süreklilik arz eden bir döngüdür. Bu sebeple belli periyotlarla sürekli yenilenmelidir. Bu çalışmada bahsedilen risklerin bazıları, gelecekte uygulanacak yeni metodolojilerin etkisiyle önemini kaybedebilecektir. Ayrıca bu çalışmada kamu kurum ve kuruluşlarının faaliyetleri açısından istenmeyen etkiler oluşturabilecek belli başlı risklere ve yine bulut bilişim mimarileri ile ilgili tehdit ve zafiyetlerin başlıcalarına yer verilmiştir. Hiç şüphesiz, bunları ve bunların yanında uygulanacak önlem ve kontrolleri artırmak ve çeşitlendirmek mümkündür. Yine bu çalışma boyunca riskler, bulut bilişim

hizmeti alan müşteri kamu kuruluşları açısından değerlendirilmiştir. Ancak, genellikle etkileri benzer olmakla birlikte, bu risklerin sağlayıcı ve kullanıcı vatandaşlar gibi diğer paydaşlar üzerinde farklı yansımaları olabilecektir. Bu anlamda, bu çalışmanın devamında diğer paydaşlar açısından ilgili risk yönetimi süreci tekrarlanabilecektir. Ayrıca teknik, kurumsal ve stratejik ve hukuksal gibi farklı alanlarda belirlenen riskler; genel bir bakış açısıyla değerlendirilmiştir. İleriki çalışmalarda, kuruluşların farklı birimlerinin sorumluluğundaki alanlarla ilgili bu risklerin, sorumlu birimin bakış açısıyla değerlendirilmesi faydalı olacaktır. Yine bu çalışmada belirlenen risklerin, kuruluşların ilgili birimlerinin varsa risk yönetim süreçlerine dâhil edilmesi, ilgili süreçlerin bu riskler için periyodik olarak uygulanması ve sonuçlarının kaydedilmesi; çalışmanın devamı niteliğindeki en önemli adım olacaktır.

KAYNAKLAR

Accenture, 2013, European Public Services - Cloud Changes the Game, http://www.accenture.com/us-en/Pages/insight-european-public-services-cloud.aspx, (06.08.2016)

Advance Software Products Group, 2013, 10 Tips for Securing Encryption Keys, http://aspg.com/10-tips-for-securing-encryption-keys/#.V--mB_CLTIU, (25.08.2016)

ALKHALIL Adel, SAHANDI Reza, JOHN David, 2013, Migration to Cloud Computing-The Impact on IT Management and Security, 1st International Workshop on Cloud Computing and Information Security, Atlantis Press, s.196-200

ALMUNAWAR Mohammad Nabil, ALMUNAWAR Hasan Jawwad, 2014, Outsourcing Computing Resources through Cloud Computing, Encyclopedia of Information Science and Technology, s.5199–5210

ANDERSON Ross J., 2008, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, ISBN: 978-0-470-06852-6

ANDRIKOPOULOS Vasilios vd., 2013, How to Adapt Applications for the Cloud Environment, Computing, s.493–535

AUBAKİROV Margulan, NİKULCHEV Evgeny, 2016, Development of System Architecture for EGovernment Cloud Platforms, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, s.253-258

BARROS Alistair P., DUMAS Marlon, 2006, The Rise of Web Service Ecosystems, IT Professional 8, ISSN: 1520-9202, s. 31-37

Benny ROCHWERGER vd., 2009, "The Reservoir Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4., s.12

BESERRA Patricia vd., 2012, Cloudstep: A Step-By-Step Decision Process to Support Legacy Application Migration to the Cloud, In Proceedings of and Evolution of Service-Oriented and Cloud-Based Systems, s.7–16

Business Software Alliance (BSA), 2016, The 2016 BSA Global Cloud Computing Scorecard

CARSTENSEN Jareed vd, 2012, Cloud Computing - Assessing the Risks (Paperback), IT Governance Publishing, UK

CHANDRAMOULI Ramaswamy, 2014, Security Recommendations for Hypervisor Deployment, National Institute of Standards and Technology, USA

Cisco, 2013, Enabling Your Journey to Government Cloud, USA

Cisco, 2015, Networking and Cloud: An Era of Change, http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/cloudcomputing/white_paper_c11677946.html, (27.08.2016)

COCHRAN Mitchell, WITMAN Paul D., 2011, Governance and Service Level Agreement Issues in a Cloud Computing Environment, Information Technology Management, s.41-55

COLES Cameron, 2011, Advantages of Cloud Computing and How Your Business Can Benefit From Them, https://www.skyhighnetworks.com/cloud-security-blog/11advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them, (25.07.2016)

Computing and Information Services Newsletter, 2015, Hipervizörler, http://cisn.metu.edu.tr/ 2011-19/sanal.php, (13.07.2016)

ÇİNTİMUR Mehmet Bilgekağan, KAYA Tolga, YILDIZ Erdinç Kadir, 2014, Bulut Bilişim Raporu, Yerel Yönetimlerde Coğrafi Bilgi Sistemlerinin Yaygınlaştırılmasına Yönelik Yol Haritasının Belirlenmesi, Türkiye

DALE Chris , BURKE Patrick J., 2012 , The E-Discovery Implications Of The Cloud, The Metropolitan Corporate Counsel, s.12

DECKER Dr. Marnix A.C., 2012, Security Framework for Governmental Clouds, The European Network and Information Security Agency (ENISA)

DPT Bilgi Toplumu Stratejisi Eylem Planı (2006-2010), 2006, Devlet Planlama Teşkilatı, http://www.bilgitoplumu.gov.tr, (08.08.2016)

DPT Bilgi Toplumu Stratejisi Eylem Planı (2015-2018), 2015, Devlet Planlama Teşkilatı, http://www.bilgitoplumu.gov.tr, (08.08.2016)

ERGİN Oğuz vd., 2012, Kamuda Bulut Bilişim, 1. Çalışma Grubu, Türkiye Bilişim Derneği Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu BiliÇim Platformu XIV, Ankara

ESKİYÖRÜK Doğan, 2007, BGYS - Risk Yönetim Süreci Kılavuzu, Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

EZZAT Eman M., EL ZANFALY Doaa S., KOTA Mohamed M., 2011, Fly over Clouds or Drive Through the Crowd: A Cloud Adoption Framework, International Journal of Computer Applications, Volume 56– No.4, s.6–11

Fokus, 2013, GoBerlin – Marketplace for Trustworthy Governmental and Business Services,www.fokus.fraunhofer.de/en/elan/projekte/national/go_berlin/index.html, (05.08.2016)

GABRIELSSON Jan vd., 2010, Cloud Computing in Telecommunications, Network service providers to offer cloud, Ericsson Review, s.29-34

GARG Abhinav, 2011, Cloud Computıng For The Fınancıal Servıces Industry, Sapient Global Markets

GENS Frank, 2009, New Idc IT Cloud Services Survey: Top Benefits and Challenges, IDC exchange, http://blogs.idc.com/ie/?p=730, (18.08.2016)

GOLDEN Bernard, 2009, The Case Against Cloud Computing, http://www.cio.com/article/2430450/cloud-computing/the-case-against-cloud-computing-conclusion.html, (15.08.2016)

GONGOLIDIS Evangelos., KALLONIATIS Christos, KAVAKLI Evangelia, 2014, Requirements Identification for Migrating e-Government Applications to the Cloud In Information and Communication Technology, Springer Berlin Heidelberg, Vol. 8407, s.150–158

Gov.Uk, 2013, Government Adopts "Cloud First" Policy for Public Sector IT, https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public sector -it, United Kingdom

Government of Spain Ministry of Finance and Public Administration, 2013, Towards a Cloud Computing Strategy in the Public Administration, https://administracion electronicagob.es/pae_Home/dms/pae_Home/documentos/OBSAE/pae_Notas_Tecnicas/201302_nota_tecnica_cloud_en.pdf, Spain

GUO Zhiyun, SONG Meina, SONG Junde, 2010, A Governance Model for Cloud Computing, Management and Service Science Conference (MASS), s.1–6

HAI Jeong Chun, 2007, Fundamental of Development Administration, Selangor: Scholar Press, ISBN 978-967-5-04508-0, Malaysia

HICKS Deron R., 2009, Chinese City Builds Public Cloud to Aid Innovation FutureGov Asia Pacific: Transforming Government + Education + Healthcare , http://www.futuregov.net/ articles/2009/sep/29/oil-rich-chinesecity-buildspublic-cloud-aid-inno/, (02.08.2016)

HOF Robert, 2016, Ten Years on, Jeff Bezos' 'Risky Bet' on Amazon Web Services Pays Off Big, http://siliconangle.com/blog/2016/03/14/ten-years-on-jeff-bezos-risky-bet-on-amazon-web-services-pays-off-big/, (13.07.2016)

HOWARD Alex, 2012, Making Dollars and Sense of the Open Data Economy, O'Reilly Radar, http://radar.oreilly.com/2012/12/making-dollars-and-sense-of-the-open-data-economy. html, (13.08.2016)

IOVAN Stefan, DAIAN Gheorghe Iulian, 2013 Impact of Cloud Computing on Electronic Government, Railway Informatics, s.71-77

JACKSON Kevin L., 2011, Implementation of Cloud Computing Solutions in Federal Agencies, http://www.forbes.com/sites/kevinjackson/2011/08/29/implementation-of-cloud-computing-solutions-in-federal-agencies-part-3-cloud-transition-lessonslearned, (22.08.2016)

JONES P., 2012, China's Growing Cloud Industry, Datacenter Dynamics, http://www.datacenterdynamics.com/focus/archive/2012/05/china%E2%80%99s-growing-cloud-industry, (10.08.2016)

KANDUKURI Balachandra Reddy, PATURI Ramakrishna V, RAKSHIT Atanu, 2009, Cloud Security Issues, Services Computing, s.517–520

KERR Kathryn, 2001, Malicious Scanning, Global Information Assurance Certification Paper, s.1-6

KHAJEH-HOSSEINI Ali, GREENWOOD David, SOMMERVILLE Ian, 2010, Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS, IEEE, s.450–457

KREBS Rouven, MOMM Christof, KOUNEV Samuel, 2012, Architectural Concerns in Multi-Tenant SaaS Applications, Karlsruhe Institute of Technology, s.2

KRESS Juergen, 2015, Cloud Computing Definition & Architecture for Cloud Service Brokers, Oracle,https://blogs.oracle.com/soacommunity/entry/cloud_computing_definition_architecture_for, (13.08.2016)

KOCHER Paul, 1996, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems, Advances in Cryptology—Crypto'96, s.104–113

KOÇ Fatih, 2008, Bgys - Varlık Envanteri Oluşturma Ve Sınıflandırma Kılavuzu, Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

KUNDRA Vivek, 2010, Cloudbook, http://www.cloudbook.net/community/contributors /vivek-kundra, (28.07.2016)

KUYORO Shade O., IBIKUNLE Frank, AWODELE Oludele, 2011, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks, s.247–255

LARSON Christina, 2013, Will Cloud Computing in China Be a Boon or Peril for Business, BusinessWeek: Technology, http://www.businessweek.com/articles /2013-09-10/will-cloud-computing-in-china-be-a-boon-or-peril-for-business, (12.08.2016)

LEWIS Grace A., 2013, Role of Standards In Cloud-Computing Interoperability, System Sciences (HICSS), s.26-34

LI Ang, 2010, CloudCmp: Comparing Public Cloud Providers, 10th Annual Conference On Internet Measurement, s.1–14

MAHMOOD Zaigham, 2015, The Advances in Electronic Government, IGI Global, Digital Divide, and Regional Development (AEGDDRD) Book Series ISSN 2326-9103, USA

MARTENS Benedikt, WALTERBUSCH Marc, TEUTEBERG Frank, 2012, Costing of Cloud Computing Services: A Total Cost of Ownership Approach, 2014 47th Hawaii International Conference on System Sciences, s.1563–1572

MATHER Tim vd., 2009, Cloud Security and Privacy, Cloud Security and Privacy, O'Reilly Media, Inc., ISBN: 978-0-596-80276-9,USA

MCKENDRICK Joe, 2011, Cloud Computing's Hidden 'Green' Benefits, http://www .forbes.com/sites/joemckendrick/2011/10/03/cloud-computings-hidden-green-benefits/, (17.08.2016)

MCKENDRICK Joe, 2013a, Cloud Computing May Save U.S. Government $20 Billion A Year (But There's More To It Than Just Cost Savings, http://www.forbes.com/sites/ joemckendrick/2013/11/20/cloud-computing-may-save-u-s-federalgovernment20billion-a-year-but-theres-more-to-it-than-just-cost-savings, (16.08.2016)

MCKENDRICK Joe, 2013b, 10 Steps to Avoid Cloud Vendor Lock-in, http://www.zdnet.com/article/10-steps-to-avoid-cloud-vendor-lock-in/, (04.09.2016)

MELL Peter, Timothy GRANCE, 2011 The NIST Definition of Cloud Computing, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145, USA

MEULEN Rob van der, PETTEY Christy, 2008, Gartner Says Cloud Computing Will Be As Influential As E-business, Special Report Examines the Realities and Risks of Cloud Computing, Gartner, USA

Microsoft, 2016, Microsoft Hizmetler Sözleşmesi, http://windows. microsoft.com/tr-TR/windows-live/microsoft-services-agreement, (28.07.2016)

Ministry of Internal Affairs and Communications of Japan (MIC), 2009, MIC Announces the Outline of Digital Japan Creation Project (ICT Hatoyama Plan), Communications News, Biweekly Newsletter of the Ministry of Internal Affairs and Communications

MITRE Institute, 2010, Risk Mitigation Planning, Implementation, and Progress Monitoring, https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems engineerin g/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring, (28.08.2016)

MOSHER Richard, 2011, Cloud Computing Risks, ISSA Preeminent Trusted Global Information Security Community, s.34-38

NEWCOMER, Eric; LOMOW, Greg, 2005, Understanding SOA with Web Services, Addison Wesley, ISBN 0-321-18086-0, USA

ONWUDEBELU Ugochukwu, CHUKUKA Benedict, 2012, Will Adoption of Cloud Computing Put the Enterprise at Risk?, Adaptive Science Technology (ICAST), s.82–85)

O'REILLY Tim, 2009, Gov 2.0: It's All About The Platform, TechCrunch, https://techcrunch. com/2009/09/04/gov-20-its-all-about-the-platform, (13.08.2016)

O'REILLY Tim, 2005, What Is Web 2.0, O'Reilly Network, http://www.oreilly .com/pub/a /web2/ archive/what-is-web-20.html, (01.07.2016)

ÖZTÜRK Hakkı, YÜKSEK Cumali, ASLAN Mustafa, 2014, Bilgi Güvenliği Politikaları Kılavuzu, Sağlık Bakanlığı Sağlık Politikaları Bilgi Sistemleri Genel Müdürlüğü, Ankara

PARKER Simon, BARTLETT Jamie, 2008, Towards Agile Government, Academic Press, s. 20-27

PERRIN Chad, 2010, Mitigating the Privilege Escalation Threat, IT Security, http://www.techrepublic.com/blog/it-security/mitigating-the-privilege-escalation-threat/, (01.09.2016)

PETTEY Christy, GOASDUFF Laurence, 2009, Gartner Highlights Five Attributes of Cloud Computing, Gartner, USA

Rackspace Catalogue, 2016, Advantages of Cloud Computing, http://www.rackspace .co.uk/ cloud-computing/advantages, (21.07.2016)

RHODY Sean, 2013, Capgemini Government Cloud Broker: A Point of View, Capgemini Consulting Technology Outsourcing, s.6

RITTINGHOUSE John W., RANSOME James F., 2010, Cloud Computing Implementation, Management and Security, Taylor and Francis Group, LLC, ISBN: 978-1-4398-0680-7, USA

ROMES Randy, 2013, The Benefits and Risks of Cloud Computing, http://www .claconnect.com/resources/articles/the-benefits-and-risks-of-cloud-computing, (25.07.2016)

ROSADO, David g. vd., 2012, Security Egineering for Cloud Computing: Approaches and Tools, IGI Global; ISBN-13: 978-1466621251 1. Edition, USA

ROUSE Margaret, 2014a, Cloud Encryption, http://searchcloudstorage.techtt.com/ definition/cloud-storage-encryption, (23.08.2016)

ROUSE Margaret, 2014b, Vendor Lock-in, http://searchconvergedinfrastructure .techtarget. com/definition/vendor-lock-in

RYAN Patrick S., MERCHANT Ronak ve FALVEY Sarah, 2011, Regulation of the Cloud in India, Journal of Internet Law, Aspen Publishers, s.7

Salesforce UK, 2015, Why Move To The Cloud? 10 Benefits Of Cloud Computing, https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html, (25.07.2016)

Service Architecture, 2015, http://www.servicearchitecture.com/articles/cloudcomputing /cloud_computing_categories.html, (05.07.2016)

SHACKLEFORD Dave, 2010, Cloud Security and Compliance: A Primer, SANS Institute Whitepaper, USA

SNIA, 2014, Cloud Data Management Interface (CDMI), http://www.snia.org/cdmi, (11.08.2016)

Softaculous Auto Installer, 2015, http://www.softaculous.com/website/images/webuzo /cloud-computing.png (23.06.2016)

STONE Greg, NOEL Pierre, 2015, Cloud Risk Decision Framework, Principles & Risk-based Decision Making for Cloud-based Computing Derived from ISO 31000

STONEBURNER Gary, 2002, NIST Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, USA

T.C. Başbakanlık, 2002, e-Türkiye Girişimi Eylem Planı, Ankara

T.C. İçişleri Bakanlığı Bilgi İşlem Dairesi Başkanlığı, 2015, İçişleri Bulut Belediye Projesi, http://www.icisleribilgiislem.gov.tr/icisleri-bulut-belediye-projesi, Ankara (11.09.2016)

T.C.Kalkınma Bakanlığı Bilgi Toplumu Dairesi, 2009, E-Dönüşüm Türkiye, Ankara

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü E-Devlet Hizmetleri Dairesi Başkanlığı, 2016, E-devlet için Genel Görünüm, T.C. Ulaştırma, Denizcilik ve Haberleşeme Bakanlığı, Ankara

Techtarget Network, 2015, Cloud Orchestrator, http://searchitoperations.techtarget.com/definition/cloud-orchestrator (09.07.2016)

Techopedia, 2016, Cloud Middleware, https://www.techopedia.com/definition/30630/cloud-middleware-software (22.07.2016)

The SageNet Team, 2015, The Risks of Poor Patch Management and How to Avoid Them, http://www.sagenet.com/Support/Blog/the-risks-of-poor-patch-management-and-how-to-avoid-them-546, (21.08.2016)

TINHOLT Dinand, 2014, Delivering on the European Advantage? How European Governments Can and Should Benefit from Innovative Public Services, European Commission, Directorate-General for Communications Networks, Content and Technology, EU

TS ISO/IEC 27000:2014 - Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Sözlük, TSE, Ankara

TSE, 2014, Bulut Bilişim Güvenlik ve Kullanım Standart Taslağı, Ankara

TURAHI Dr. David, 2013, Security and Privacy: Can we trust the cloud?, Ministry of Information and Communications Technology (ICT) Information Technology and Information Management Services, USA

TUSANOVA Adela, 2012, Decision-Making Framework for Adoption of Cloud Computing, 12th Scientific Conference of Young Researchers, s.110-112

Türkiye Bilişim Derneği, 2012, Kamuda Bulut Bilişim, Ankara

ULREY Sue, 2014, The Benefits and Risks of Cloud Computing, http://nexia.com/ publications/global-insight/archive/2014/global-insight april2014/technology /the-benefits-and-risks-of-cloud-computing, (26.07.2016)

VAJDA Andras, 2012, Cloud Computing and Telecommunications: Business Opportunities, Technologies and Experimental Setup, World Telecommunications Congress (WTC), s.11-18

WARREN Katy, 2015, Federal Cloud Security, MITRE Corporation, s.8

WEST, Darrel M.,2010, Saving Money Through Cloud Computing, Governance Studies at Brookings, USA

Zacks Equity Research, 2012, Accenture to Build French G-Cloud, http://www.nasdaq.com/article/accenture-to-build-french-gcloud-analyst-blogcm114808, (10.08.2016)

ZWATTENDORFER Bernd, TAUBER Arne, 2013a, The Public Cloud for E-Government International Journal of Distributed Systems and Technologies, s.1–14

ZWATTENDORFER Bernd vd., 2013b, Cloud Computing in E-Government across Europe, In Technology-Enabled Innovation for Democracy, Government and Governance, Springer, s.181–195

ETİK KURALLARA UYGUNLUK BEYANI

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Çevre ve Şehircilik Uzmanlığı Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Çevre ve Şehircilik Bakanlığı tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

17/01/2017

Hakan KILIÇ

ÖZGEÇMİŞ

1982 yılında Vakfıkebir'de doğdu. İlk, orta ve lise öğrenimini Trabzon'da tamamladı. 2006-2009 yılları arasında Gıda, Tarım ve Hayvancılık Bakanlığı Personel Genel Müdürlüğü'nde Memur olarak çalıştı. 2009 yılında Ortadoğu Teknik Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü'nden mezun oldu. Aynı yıl Eti Maden İşletmeleri Genel Müdürlüğü emrine Mühendis olarak atanarak, 2014 yılına kadar bu kurumda görev yaptı. 2014 yılında Çevre ve Şehircilik Bakanlığı'nda Çevre ve Şehircilik Uzman Yardımcısı olarak göreve başladı. Halen Çevre ve Şehircilik Uzman Yardımcısı olarak çalışmaktadır. Evli ve iki çocuk babasıdır.